### PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2003-101533

(43)Date of publication of application: 04.04.2003

(51)Int.CI.

H04L 9/32 G06F 15/00

H04L 9/08

(21)Application number: 2001-292581

(71)Applicant : TOSHIBA CORP

(22)Date of filing:

25.09.2001

/=0\r

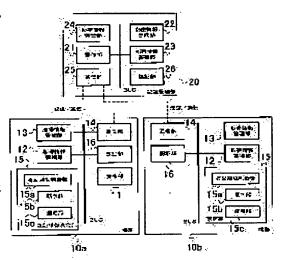
(72)Inventor: YAMAGUCHI KENSAKU

NAKAKITA HIDEAKI HASHIMOTO MIKIO

## (54) DEVICE AUTHENTICATION MANAGEMENT SYSTEM AND METHOD THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent occurrence of a situation where each device cannot start communication with each other when there is a difference in the expiration time of the effective period for a common key used by each device in authentication among devices. SOLUTION: A device authentication management system obtaining a predetermined secret information from a authentication management means manages the secret information, and conducts authentication for communication with other devices using the secret information. The authentication management means comprises a generation means for generating the secret information having a first authentication information for communication between the authentication management means and the device, and a second authentication information for communication between the device and other devices, a first authentication means for conducting authentication for communication with the device using the first authentication information



generated by the generation means, and a first transmission means for transmitting the second authentication information, based on authentication by the first authentication means.

퐳 ধ 弫 华 噩 4 (22) (19) 日本国格許庁 (JP)

特開2003-101533 (11)特許出國公開卷号

€

(P2003-101533A)

(43)公開日 平成15年4月4日(2003.4.4)

51) Int.Cl.		数别記号	1 F			17	テーマコード(参考
H04L	38/35		G06F 1	12/00	3300		5 B 0 8 5
G06F	15/00	330	H04L	00/6	675A	ι	J 104
H04L	80/6				601B	_	
					601E		
					6 7 5 D	_	
			審查請求	米部分	解状型の数11 01	0	& ₩

Î

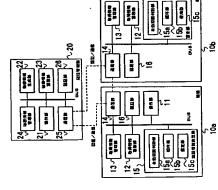
(21)田岡神中	(本版2001 - 292581(P2001 - 292581)	(71) 田間人 000003078	000003078
			株式会社東芝
(22)出版日	<b>平成13年9月25日(2001.9.25)</b>		東京都港区芝浦一丁目1番1号
		(72) 免明者	山口海外
			神奈川県川崎市幸区小向東芝町1番地 株
			式会社東芝研究開発センター内
		(72)発明者	中北 英明
			神疾川県川崎市幸区小向東芝町1番地 株
			式会社東芝研究開発センター内
		(74)代理人	(74)代理人 100083806
			井理士 三好 秀和 (外7名)
			最終質に取く

# (54) 【発明の名称】 機器関配管理システム及び機器認証管理方法

行われる通信を開始することができなくなることを防止 【磔題】 各機器が、各機器との間の認証に用いる共通 腱の有効期限の終了時刻に差がある場合に、各機器間で

「解決手段」 所定の秘密情報を管理する認証管理手段 から前記秘密情報を取得した機器が、取得した跋秘密情 **魚を用いて他の機器との間で通信をするための認証を行** が、前記器監管理手段と前記機器との間で通信を行うた う機器路証管理システムであって、前記器証管理手段

を行うための第二認証情報とを有する前記秘密情報を生 路監情報を用いて、前記機器との間で通信をするための めの第一點監督報と、前記機器と他の機器との間で通信 成する生成手段と、前配生成手段で生成された前記第一 路証を行う第一認証手段と、前記第一器証手段の認証に 基づいて前配第二陽監情報を送信する第一通信手段とを 介することを特徴とするものである。



(請求項1) 所定の秘密情報を管理する認証管理手段 から前記秘密僧報を取得した機器が、取得した政秘密情 **報を用いて他の機器との間で通信をするための認証を行** う機器陽監管理システムであって、

前記器監管理手段は、

第一認証情報と、前記機器と他の機器との間で通信を行 前記認監管理手段と前記機器との間で通信を行うための うための第二器監情報とを有する前配秘密情報を生成す る生成手段と、

前記機器との間で通信をするための認証を行う第一認証 前記生成手段で生成された前記第一路証情報を用いて、

前記第一點紅手段の陽缸に払ろいて前記第二陽距价報を

送信する第一通信手段とを有し、

報を用いて、前記第一認証手段との関で通信をするため 前記器証管理手段から予め取得してある前記第一路監督 の器証を行う第二器証手段と、 抗的第二路駐街の路路に基めいて拒犯第一通信中段から 前記第二點監情報を受信する第二通信手段とを有するこ とを特徴とする機器認証管理システム。 【開水項2】 請水項1に記載の機器認証管理システム

前記第二器証手段は、前記第二通信手段で受信した第二 認証情報を用いて、前配他の機器との間で通信をするた めの認証を行う機能を有し、

て、前記他の機器との間で通信を行う機能を有すること 前的第二通信手段は、前配第二認証手段の認証に基づい を特徴とする機器認証管理システム。

[請求項3] 請求項1又は請求項2に記載の機器認証 管理システムであって、

前配第二器証付報は、該第二器証付報を確別するための 韓別子と、前配第二路監備報を使用することができる有 効期限情報とを有することを特徴とする機器認証管理シ 【制水項4】 請水項3に配載の機器陽話管理システム **かをした、拒配報路は、** 

る前記織別子を取得し、その取得した前記職別子と、前 前記他の機器が有する複数の前記第二器配情報に含まれ 記機器が有する複数の前記第二認証情報に含まれる前記 観別子との間で共通する前記職別子を抽出して、その抽 紋織別子に対応する前記有効期限情報に基ろいて、故有 効期限情報に対応する一つの前配第二路監算報を選定す 出した前記職別子に対応する前記第二路開拾報のうち、 る第一選定手段と、

前記第二陽証手段は、前記第一選定手段で遵定された第 るための認証を行う機能を有することを特徴とする機器 ||怒暗拉数に揺んにん、 点的色の破路 | の回 の通信を | 認証管理システム。

**参照2003-101533** 

3

[開水項5] 開水項2又は開水項3に配破の機器制能

价税を取得した時間を、前配第二路配价税に付加する時 前記第二通信手段が前記器監管理手段から前記第二路監 作型システムであった。 間付加手段と、

伯的祭士婦院は他の中から、年加された白的時間に成る 情報を複数取得し、その前記時間が付加された複数ある いて、破時間に対応する一つの前記第二路監信権を適定 前記時間付加手段で前記時間が付加された前記第二路艦 する第二箇定手段と、 9

的第二路話行程に払んいた、自動他の複雑との向い路距 前配第二陽配手段は、前配第二箇定手段で適定された前 を行う機能を有することを特徴とする機器関脳管理シス 74.

【開水項6】 開水項2に配載の機器陽低管理システム 前記第二路監備報を所定の周期毎に生成する前配生成年

情報を複数取得し、その複数取得した前配第二點配信機 の個数が所定の個数を組えたときは、取得した複数ある **荷配第二點能位後のうちのいずれかを何除する知三違定** 前記生成手段で所定の周期毎に生成された前記第二陽監 **平段とを有することを特徴とする機器認証管理システ** 20

から前記器監督報を取得した機器が、取得した破器監督 【精水項7】 所定の陽証情報を管理する陽証管理事段 報を用いて他の機器との肌で通信をするための路証を行 **シ 職器 監禁 監禁 単力 法 ひもった、** 

第一路監備報と、前記機器と他の機器との間で通信を行 前配路監管理手段と前配機器との間で通信を行うための うための第二陽監情似とを有する前記器監情報を生成す 前配陽監管理手段は、 30

生成された前記第一路監督報を用いて、前記機器との調 で通信をするための協能を行うステップと、 るステップと、

**世記破略との国で通信をするための観覧に続
といて信** 第二路証情報を送信するステップとを有し、

前記錫斯作用手段から予め取得してある前配類一點配置 報を用いて、前記認証管理手段との間で通信をするため 信記概器は、 9

伯記認証管理手段との回で通信をするための認証に払う いて、位的認能作単手段から何的第二認能は個を収信す るステップとを有することを特徴とする機器陽配管型方 の駱駝を行うステップと、

って、何記機器は、伯記認証管理年段から受信した第二 [韵水項8] 静水項7に記載の機器器配管則方法であ **路証付報を用いて、何配他の機器との回で通信をするた** めの悶肌を行うステップと、

前配他の機器との間で通信をするための路話に基づい

20

-2-

[請求項9] 請求項7又は請求項8に記載の機器認証 **竹理方法であって、前記第二路監督報は、前記第二路監 情報を職別するための観別子と、前記第二器証情報を使** 用することができる有効期限情報とを有することを特徴 とする機器認証管理方法。

【請求項10】 請求項9に記載の機器器監管理方法で **あった、拒記機器は、**  前記他の機器が右する複数の前配第二器駐情報に含まれ る前記機別子を取得し、その取得した前記機別子と、前 観別子との間で共通する前記観別子を抽出して、その抽 記機器が有する複数の前記第二認証情報に含まれる前記 核権別子に対応する前配有効期限情報に基づいて、該有 効期限情報に対応する一つの前記第二點指情報を選定す 出した前記権別子に対応する前記第二器監督報のうち、 るステップと、

韓定された前記第二路監督報に基づいて、前記他の機器 との間で通信をするための認証を行うステップとを有す ることを特徴とする機器踢駐管理方法。

[請求項11] 請求項8又は請求項9に記載の機器賜 証管理方法であって、前配機器は、

前記器証管理手段から前記第二器証情報を取得した時間 を、前配第二點証情報に付加するステップと、

との間で認証を行うステップとを有することを特徴とす その前記時間が付加された複数ある前記第二路監情報の 中から、付加された前配時間に基ろいて、鞍時間に対応 衛定された前記第二器監督與に基づいて、前記他の機器 前記時間が付加された前記第二陽監情報を複数取得し、 する一つの前記第二點監情報を選定するステップと、 5機器器監管理方法。

[発明の詳細な説明]

[1000]

[発明の風する技術分野] 本発明は、所定の秘密情報を 管理する陽証管理手段から前記秘密情報を取得した機器 が、吸得した秘密情報を用いて他の機器との間で通信を するための認証を行う機器認証管理システム及び機器認 証管理方法に関する。

[0002]

1)間の接続を中心として、ネットワーク化が進行してい ば、この無級LAN化によれば、有級LANに無線基地局を接 院し、この基地局へ複数の携帯型パーンナルコンピュー 【従来の技術】近年のLAN(Local Area Network)技術の 発速に伴い、オフィス環境では、PC(Personal Compute る。このような有線LMの普及の一方では、有級LMの一 部分を無線で置換する無線LAN化も進んでいる。例え タを無級で接続することができる。

が、有級LANにイーサネット(登録商標)接続されてい [0003] そして、乾特型パーソナルコンピュータ

るパーソナルコンピュータとの国で無数により通信接続

20

タのファイルを編集することができる。これにより、携 を行い、その通信接続が行われたパーソナルコンピュー **帯型パーソナルコンピュータは、有線LANへ無線アクセ** スを行っていることになる。

や赤外線などを利用するので配線敷設が不要なこと、ネ ットワークの新散やレイアウト変更が容易なことなどが [0004] また、基地局と携帯型パーソナルコンピュ -タの部分との間は、無极LANを形成していることにも なる。このような無級LANの利点は、伝送路として電波

挙げられる。

01

仕様の伝送速度は、1~2Mbpsのものと11Mbpsのものとが 【0005】無級LANの導入は、IEEE 802.11の標準化に よって、柏車がかかっている。IEEE802.11では、1997年 に2. 4GHz 帯の無線LAN仕様を、1999年に5GHz 帯の無線LAN 仕様を、それぞれ完成させている。2.4GHz帯の無数LAN が、各社から発売されるようになり、基地局や無線PCカ あり、さらに20Mbpsを超える仕様が現在検討中である。 设近、この2.4GHz帯の無級LAN仕様に準拠した製品 ードが、普及価格特に入りつつある。

かつ、より高速な伝送速度が容易に見込めるため、次世 は、20~30Mbpsを実現できる。また、5GHz帯は、2.4GHz の通信機能を有するチップの価格が、1チップ35ドルで2 代の無験LAN仕様と期待されている。 最近では、5GHz 特 帯とは異なり、現在はほぼ未使用な通信周波数帯域で、 【0006】一方、5GHz帯の無線LAN仕様の伝送速度 20

001年中に発売予定というベンチャ企業も現れており、5 電話業界や家電業界やPC業界を巻き込んで、あらゆる機 による通信方式を採用したチップの価格は1チップ5ドル 広い業種の約2000社から賛同を得ていること、Bluetoot よる通信方式を用いた無線機器は、世界的に普及すると [0007] 更に、Bluetoothによる通信方式が、携帯 路に搭載されようとしている。このBluetoothによる通 倡方式も2.4GHz帯の無線システムであるが、Bluetooth 程度という低コストと、Bluetoothによる通信方式は幅 hによる通信方式を用いた無線機器は製品化と直結した 標準作成活動を行っていることなどから、Bluetoothに H2件で行われる通信も身近になりつつある。

30

でなく、一般家庭にも進んでいくものと考えられる。特 るに伴いこれらの技術の使用範囲は、オフィス環境だけ [0008] 以上のような状況から、無敏機器が普及す 見込まれている。

40

に、家庭内において配線敷設が不要となる点は、オフィ

ス環境の場合よりもさらに大きな利点である。

ライバシの保護が問題となりやすい。無線機器は、家の 【0009】しかし、無線による操作は容易な反面、無 外から、その無紋機器が勝手にコントロールされること 吹いは、無紋機器内にあるデータが壊されたりする可能 **線機器間の接続は、ケーブル接続などの場合のように明** 示的な接続ではないという特徴から、セキュリティやブ や、その無線機器から個人的な情報が盗まれることや、

タイム接続から常時接続に移行しつつあるが、これに伴 とが一般的になると、郑三者が、ファイアウォールを回 避し、無傚ネットワークインタフェースを軽白して、パ [0010] また、インターネットでの接続は、パート い無数ネットワークインタフェースで常時接続されるこ ーソナルコンピュータに進入する可能性がある。

**紫米のコンピュータウイルスに関連した報道やテレビ番** 【0011】 叉に、一般家庭ユーザは、弦感やセキュリ 組などで多少の知識を得られるような状況の中では、な ティに関連する脅威が必要であることを、コンピュータ んとなく不安を抱くものと想像される。

て、専門家を雇うなどして対策を打つことが比較的容易 つ、これらのソフトウエアを継続して更新することが必 望みにくいものである。このため、安庭内で無線機器を 【0012】ビジネス原境では、このような脅威に対し **要となるが、家庭環境では、このようなことは一般的に** 使用する際には、外部から盗聴などをされないようにす であり、IPSECやファイヤウォールなどを実数して、か るためのセキュリティ管理を充実する必要がある。

先ず、各機器のセキュリティを被括的に管理する認証管 リティを行うには、セキュリティ管理を希望する各機器 ティ管理を希望するための登録を行った各機器は、認証 管理部との間で無線ネットワークを形成し、所定の有効 れ、第三者の機器から監曝されないようにすることがで 理部を設置する。そして、認証管理部が各機器のセキュ が路監管理部に登録を行う。この路監管理部にセキュリ 【0013】この家庭内でセキュリティ管理するには、 期限内だけ、認証管理部のセキュリティ管理下に置か

家庭内の無線ネットワークに接続される危険性を減らす 【0014】但し、この有効期限は、機器が認証管理部 から付与される認証情報を使用することができる期間で 定期的に認証管理部に対して上配有効期限の更新を行う 必要がある。このように認証情報の有効期限を設定する のは、機器が未続的に家庭内無線ネットワークに接続さ れないようにする必要があること、この機器が他者へ額 渡され、廃棄されたりしたときでも、ある時点でセキュ リティ管理の有効期限が切れることによって、不用意に あり、機器は、認証情報の有効期限を更新するために、 ことが可能なためである。

**認証管理部Aのセキュリティ管理下で通信を行うために** [0015] 具体的には、図25に示すように、認証管 **型部Aは、機器10 a 及び機器10 cのセキュリティ管理** 0 cのセキュリティ管理を行うものである。一方、閲証 管理部Aは、屋外の機器10b及び隣家の機器10fの セキュリティ管理を行わないようにし、更に、賜監管理 部Bは、屋外の機器106のセキュリティ管理を行わな いようにする。このA次の機器10a及び機器10cが を行い、更に、認証管理部Bは、機器104及び機器1

る無数ネットワーク(図25中の点数の範囲内)の範囲 県部A(又はB)は、昭監管県部A(又はB)が形成す 内で、特定の機器10n 及び機器10cのセキュリティ を行うことにより実行することができる。また、陽証管 は、認証管理部Aから付与された認証情報を用いて通信 **育里を行うことができる。** 

**参照2003-101533** 

€

[発明が解決しようとする瞑題] しかしながら、セキュ [0016]

**で管理されているものであるが、無様ネットワークの危** 囲内に複数の機器が存在する場合は、各機器回で同一で あるとは限らない。一般に有効期限の終了時刻が各機器 ち、片方の機器の方が先に新しい有効期限を更新しよう 無様ネットワークを形成する範囲内に存在する各機器画 とする場合があること、各機器の持つ時計の時刻が全く リティ管理を行うことができる有効期限の終了時刻は、 匠で回しかない配信としては、宮水ば、川の裏路のウ 同一ではないことなどがあるためである。

ことは避けられない。このため、機器川で協密健の行効 有効期限を判断する場合は、たとえある時点で時間の時 **설が正確であったとしても、自機の内部に在するCPU** などの構造上、時間が特米的に進んだり、遅れたりする 世限の国格特語が同一であったかしたも、全破路の海豚 雌の有効期限は、将来的に同一時刻に終了しない場合が 【0017】また、各機器が、自機の持つ時計の時刻で

【0018】 更に、家庭で使われる各機器は、必ずしも **名時代前が入っているとは限らないため、各機器の軌弧** が入っていないときには、次に電脳が投入されるときま で認証情報の更新を受けることができない。 この場合に は、他級が投入されてから陽監情報の更新を受けるまで の遊延が発生し、その間は他の機器と異なる陽話情報を は、酩酢情報の更新を受けることができなかった機器

る秘密盤と共通している場合であっても、上記より将来 【0019】従った、機器は、鬼時点で他の機器が有す 的に他の機器が右する秘密鍵と共通しなくなる場合があ り、自機が有する秘密館を用いて他の機器との間で通信 を行うことができなくなる可能性がある。 持つ場合がある。

が揃っていなければ通信が中断される。 また、IEEE 8 02.11無QLANのようなプロードキャスト型の無線方式を ことは困難であるが、それら会ての機器が同じ陽脈情似 [0020] 各機器は、上配各機器が有する有効期限の 棒丁時刻に遊がある場合は、他の機器間で通信の開始を することができない、 吹いは他の機器間が行っている通 るので、河方の複雑三で粉幣信角を更新するタイミング 用いた機器は、通信に参加している機器の数を特定する を保存していない限り、通信が一部中断されてしまう可 **弁、ギムソ下・ギムソド医(複略医)の通伝や作りたい** 信が途中で中断されてしまうなどという問題が発生す る。例えば、Bluetoothによる無線方式を用いた機器 8

【0021】そこで、本発明は以上の点に鑑みてなされ たもので、各機器が、各機器に有する秘密壁の有効期限 の終了時刻に遊がある場合に、各機器間で行われる通信 を開始することができなくなることを防止する機器認証 管理システム及び機器管理方法を提供することを課題と

[0022]

留を解決すべくなされたものであり、請求項1に係る発 第一器駐手段と、前部第一器駐手段の器館に基づいて前 監管理システムであって、前記器監管理手段が、前記器 鉱材似と、前館機器と他の機器との間で通信を行うため するための認証を行う第二認証手段と、前記第二認証部 復を受信する第二通信手段とを有することを特徴とする 明は、所定の秘密情報を管理する認証管理手段から前記 監管理手段と前記機器との間で通信を行うための第一認 の第二點証情報とを有する前記秘密情報を生成する生成 年段と、前記生成手段で生成された前記第一路駈情報を 用いて、前記機器との間で通信をするための認証を行う 紀第二部証情報を送信する第一通信手段とを有し、前記 機器が、前距路監管理手段から予め取得してある前配第 一路監督報を用いて、前配第一路監手段との間で通信を の認能に基といれ控制終一通命手収かの推問終川認能控 【既囿を解決するための手段】本願に係る発明は上記課 86密情報を取得した機器が、取得した故秘密情報を用い て他の機器との間で通信をするための認証を行う機器器 ものである。

用いて認証管理手段との間で通信をするための認証を行 うので、何配第一路監督報を有しなければ路証管理手段 との回の通信を行うことができない。このため、鞨監管 有しない機器からの不正なアクセスを排除することがで 機器は、錫缸管理手段から子め取得した第一踢缸情報を **理手段は、第一認監情報を有していない機器との間では** 通信を行わないようにすることができ、第一踢監情報を [0023] このような粉氷項1に係る発明によれば、

[0024]また、粉水項2に係る発明は、粉水項1に 鉛板の機器器監管型システムであって、前記第二器監手 て、前配他の機器との何で通信をするための器能を行う 機能を有し、前記第二通信手段が、前記第二器証手段の 路配に基づいて、前記他の機器との間で通信を行う機能 段が、前記第二通信手段で受信した第二認証情報を用い を有することを特徴とするものである。

め、認証管理手段は、第一認証情報を有していない機器 豊器は、第一認証情報を有していなければ、認証管理手 段との間で通信を行うことができず第二路証手段を取得 することができないので、第一認証情報を有していない 機器は、錫監管理手段から他の機器との間で通信を行う ための第二認証情報を取得することができない。 このた 【0025】このような創水項2に係る発明によれば、

には第二認証情報を送信しないので、第一認証情報を有 も、前配不正要求をした機器に第二路証情報を送信しな しない機器から第二路監督報の不正要求があったとして いようにすることができる。

介して無線ネットワークを形成した各機器は、第二點配 秘密文書などの情報データが第二點監情報を有しない機 【0026】また、第二認証情報を有する機器は、第二 認証情報を用いなければ他の機器との囲で通信を行うこ とができないので、第二路監情報を有する他の機器との を形成することができる。このため、第二路証情報を媒 間では、その第二路監情報を媒介して無線ネットワーク 情報を有しない機器からの通信を排除することができ、 器に溢れることがない。

9

は請求項2に記載の機器認証管理システムであって、前 配第二路監情報が、該第二器監備報を職別するための職 別子と、前記第二陽証情報を使用することができる有効 [0027] また、請求項3に係る発明は、請求項1又 **切限情報とを有することを特徴とするものである。** 

第二點監督報には、第二點監督報の有効期限が含められ **娘の有効期限が切れれば第二陽監情報を有する機器との** ているので、第二認証情報を媒介して無線ネットワーク を形成した各機器は、第二路監情報の有効期限が切れた る。また、第二認証情報を有する機器が盗躍された場合 であっても、その機器を盗嫌された機器は、第二點証付 [0028] このような額求項3に係る発列によれば、 機器を前記無数ネットワークから排除することができ **川で通信を行うことができないこととなる。** 20

た各機器は、無線ネットワークに属する機器が監鐘され 証情報の有効期限が切れれば、その路壁された機器を無 **袋ネットワークから排除することができるので、無線ネ** 【0029】このため、上記無線ネットワークを形成し た場合であっても、その盗難された機器に有する第二器 ットワーク内の信報データがいっまでも外部に溢れ出て しまうことを防ぐことができる。

前記録別子を取得し、その取得した前記職別子と、前記 観別子に対応する前配有効期限情報に基ろいて、酸有効 [0030] また、額水項4に係る発明は、額水項3に 記載の機器器監管理システムであって、前記機器が、前 配他の機器が右する複数の前記第二器証情報に含まれる 機器が有する複数の前記第二點監備報に含まれる前記職 別子との回で共通する街記観別子を抽出して、その抽出 した前記職別子に対応する前記第二器証情報のうち、該 期限情報に対応する一つの前部第二路能情報を確定する 第一通定手段と、前記第二點監手段が、前記第一選定手 段で選定された第二器監信権に基づいて前記他の機器と の間で通信をするための認証を行う機能を有することを 特徴とするものである。

各機器は、強定手段が、他の機器が有する複数の第二器 証价額に含まれる磁別子を取得し、その取得した鐵別子 [0031] このような請求項4に係る発明によれば、

20

別子に対応する有効期限情報に基づいて数有効期限情報 に対応する一つの荷部第二略階位数を確定することがで あっても、各機器に共通の第二器監情報を遵ぶことがで と、機器が有している複数の第二器語情報に含まれる鍵 別子との回で共通する前記観別子を抽出して、その抽出 した前記権別子に対応する第二略配付権のうち、前記職 きるので、各機器に複数の第二器証情報を有する場合で

[0032] また、精水項5に係る発明は、開水項2又 は結果反当に記載の機器認証管理システムがあった。信 前記第二路監信報を複数取得し、その前記時間が付加さ れた複数ある前配第二陽監情報の中から、付加された前 配第二通信手段が前記陽監管理手段から前配第二陽監備 報を取得した時間を、前配第二路証情報に付加する時間 付加手段と、前記時間付加手段で前記時間が付加された 的時間に成んでん、数時間に対応する一つの世間符二時 が、前記第二選定手段で強定された前記第二路転情報に 払ろいて、何記色の機器との固で認覧を行う機能を有す 証情報を適定する第二選定手段と、前記第二認証手段 ることを特徴とするものである。

**呼吸かの祭川路暦拾数を収得した時刻)に揺んされ、哲** 遺定手段が、時間付加手段で付加された時間(認証管理 で、第二點監督報の有効期限情報だけでなく、前記時間 を用いることによっても第二略監情報を選ぶことができ [0033] このような粉氷項5に係る発明によれば、 配時間に対応する第二認証情報を選ぶことができるの

を所定の周期毎に生成する前配生成手段と、前配生成手 【0034】また、額米項6に係る発明は、鉛水項2に配 娘の機器路監管理システムであって、前記第二器監情報 段で所定の周期毎に生成された前配第二陽監情報を複数 取得し、その複数取得した前配第二點監情報の個数が所 定の個数を超えたときは、取得した複数ある前配第二略 証情報のうちのいずれかを削除する第三路定手段とを有 することを特徴とするものである。

第三選定手段が、生成手段で所定の周期毎に生成された 第二路証情報を複数取得し、その複数取得した第二路証 情報の個数が所定の個数を超えたときは、取得した複数 ある前配第二路証情報のうちのいずれかを削除すること ができるので、機器は、第二認証情報の有効期限を管理 する必要がなくなり、更に、有効期限を管理するための 【0035】このような額水項6に係る発明によれば、 時間管理部(図示せず)を設ける必要がない。

他の機器との間で通信を行うための第二路監情報とを有 [0036] また、額水項7に係る発明は、所定の認証 **竹報を管理する陽証管理手段から前記陽証情報を取得し** た機器が、取得した該路監督報を用いて他の機器との間 で通信をするための路証を行う機器器監管理方法であっ て、前配陽監管理手段が、前配陽監管理手段と前記機器 との間で通信を行うための第一認証情報と、前配機器と

**参照2003-101533** 

9

と、前記器監管県手段との間で通信をするための器証に するための認能に扱ういた信託祭二昭県位位を送信する 子を取得してある前記第一點監情報を用いて、前記點証 払ろいて、何智智能管理手段から何配第二點配位和を受 ステップとを有し、前記機器が、前記路監管理手段から する何配陽証情報を生成するステップと、生成された値 **記算一路駐付租を用いて、信配機器との間で通信をする** ための陽龍を行うステップと、順配機器との間で通信を 作用手段との回ぐ通信をするための結婚を行うステップ 信するステップとを有することを特徴とするものであ

9

うので、前配第一路監信権を有しなければ陽監管県手段 との間の通信を行うことができない。このため、賜監督 機器が、認覧管理手段から予め取得した第一認能信仰を 用いて陽証管理手段との間で通信をするための陽配を行 理手段は、第一路監信仰を有していない機器との仰では 面信を行わないようにすることができ、第一路監情報を 行しない機器からの不正なアクセスを排除することがで [0037] このような制水項7に係る発列によれば、

[0038] また、額水項8に係る発明は、額水項7に 記載の機器認証管理方法であった、何記機器が、前記器 **監管理手段から受信した第二路監督報を用いて、前記他** と、前院他の機器との間で通信をするための路底に基づ いて、位配色の機器との向で通信を行うステップとを右 の機器との回で通信をするための認能を行うステップ

20

することを特徴とするものである。

第二路証价報を介する他の機器との回では、その第二路 監骨組を媒介して無線ネットワークを形成することがで きる。このため、筑二路証情報を媒介して無礙ネットワ からの道信を排除することができ、秘密文章などの情報 データが第二陽監督報を有しない機器に顕れないように 一クを形成した各機器は、第二器証情報を有しない機器 第二路証付報を有する機器が、第二路証付報を用いなけ [0039] このような翻氷項8に係る発列によれば、 れば他の機器との回で通信を行うことができないので、

は韵水項8に記載の機器陽証管則方法であって、前記第 [0040] 宝九、翻水斑9に係る発明は、翻水斑7又 子と、血配第二陽監督権を使用することができる有効期 二路証符報は、前配第二路証符組を徴別するための職別 限情報とを行することを特徴とするものである。 することができる。 Ş

**であっても、その機器を強躁された機器は、折二點點指** 第二陽龍情報には、第二陽龍情報の有効期限が含められ を形成した各機器は、第二路監信組の行効期限が切れた る。また、第二路証价與を有する機器が監難された場合 **たいるので、紅川観覧信仰を繋介した熊様ネットワーク** 【0041】このような結氷項9に係る発明によれば、 機器を信配無数ネットワークから排除することができ

類の有効期限が切れれば第二點能情報を行する機器との

限位権に対応する一つの前部第二部語信仰を適定するス テップと、遠定された前配第二路監骨限に基づいて、前 た前記蔵別子に対応する前記第二器監算輯のうち、鞍鸛 四半に対応する信託在後世段は他に成ること、媒在後期 配他の機器との間で通信をするための認証を行うステッ [0042] また、翻水項10に係る発明は、翻水項9 **に配破の機器器証管理方法であって、前記機器が、前記** 他の機器が右する複数の前配第二器監備報に含まれる前 記録別子を取得し、その取得した前記鐵別子と、前記機 器が有する複数の前配第二點証借倒に含まれる前配額別 子との回で共通する伯記韓別子を抽出して、その抽出し プとを有することを特徴とするものである。

**する有効期限情報に貼るいて数有効期限情報に対応する** まれる韓別子を取得し、その取得した韓別子と、機器が ば、機器が、他の機器が有する複数の第二點配情報に含 で共通する前記模別子を抽出して、その抽出した前記模 別子に対応する第二陽監督権のうち、前部職別子に対応 有している複数の第二點監督報に含まれる臨別子との間 各機器に複数の第二器脂情報を指する場合であっても、 一つの伯配第二総証情報を違定することができるので、 [0043] このような額収項10に係る発明によれ 各機器に共通の第二點監督報を選ぶことができる。

中から、存加された値部時間に基ろいて、数時間に対応 する一つの前配紙二點監督報を強定するステップと、選 機器が、前記器監管理手段から前記第二器監情報を取得 定された前部第二路監督権に基づいて、前記他の機器と の間で路証を行うステップとを有することを特徴とする [0044] また、請水項11に係る発明は、請水項8 又は請求項9に記載の機器認証管理方法であって、前記 その前記時間が付加された複数ある前記第二器監督報の した時間を、前配第二路監情報に付加するステップと、 前部時間が付加された前部第二路監信報を複数取得し、 ものである。

**手段から第二器監信権を収得した時刻)に基乙いた、前** を用いることによっても第二認証情報を遵ぶことができ ば、機器は、時間付加手段で付加された時間(路証管理 で、郑二路監督他の在参規限信仰だけでなく、他記時間 [0045] このような静水項11に係る発明によれ 記時間に対応する第二総監督報を強ぶことができるの

## [0046]

【発明の実施の形像】 [第一実施形態]

5. 同図に示すように、機器認証システムは、所定の税 密情報を管理する認証管理部20から秘密情報を取得し (機器器証管理システムの構成) 本発明の実施形態につ **いて図面を眷照しながの説明する。図2は、本尖施形態** た機器10aが、取得した秘密情報を用いて他の機器1 0 b との間で通信をするための認証を行うものである。 に係る機器認能システムの内部構造を示したものであ

【0047】ここで、認証管理部20は、認証管理部2 0と機器10との間で通信を行うための第一認証情報

第二路証情報からなる秘密情報を生成する秘密情報生成 部22と、秘密情報生成部22で生成された第一路距情 行う認証部26と、認証部26の認証に基ろいて第二路 と、機器10と他の機器10との間で通信を行うための **報を用いて、機器10との間で通信をするための認証を** 胚情報を送信する通信部25とを備えている。 [0048]また、機器10は、認証管理部20から予 め取得してある第一総監情報を用いて、認証部26との **川で通信をするための認証を行う認証部16と、認証部** 16の認証に払ん、大通信部25かの第二認能位数を受 留する通信部14とを備えている。

た各機器10g~10cが、取得したマスタ健Ma~Mc 報データの送受信を行いたい各機器10 a ~10 c との 【0049】 即ち、機路認証システムは、図1に示すよ 設証管理部20から取得し、その共通観Kを取得した各 **問か認証をする。この共通徴Kを用いて認証が成功した** 各機器10a~10cは、認証が成功した各機器の相互 うに、認証管理部20からマスタ鍵Mョ〜Mcを取得し を用いて、各機器10a~10cに共通する共通鍵Kを 機器10g~10cは、取得した共通盤Kを用いて、情 川で情報データを送受信することができる。

[0050]上記マスタ鏈Mは、認証管理部20と機器10 との間で通信を行うための第一器監開報 (暗号キー) で の一部であり、機器10と他の機器10との間で通信を ある。また、共通健Kとは、第二路監情報(認証情報)

行うための時号キーを意味するものである。

0との間で通信を行うための第二認証情報であり、例え ば、各機器10との間で共通の暗号器証を行うための共 **通数K (時号キー) と、認証情報を職別するための職別** 子と、認証情報の有効期限を示す有効期限情報とを有し ている。更に、秘密情報は、第一點監情報と第二點監情 【0051】また、認証情報は、機器10と他の機器1

【0052】図2に示すように、本実施形態に係る機器 **数証システムは、機器10と、認証管理部20とを有し** 粗とを含めたものを意味する。

の秘密情報を取得し、その取得した秘密情報を用いて他 【0053】前記機器10は、認証管理部20から所定 の機器 10との間で通信をするための認証を行うもので あり、本実施形態では、操作部11と、取得情報蓄積部 12と、取得情報管理部13と、通信部14と認証情報 決定部15と、認証部16とを有している。

40

[0054]操作部11は、情報データなどの入力を行 ジョイスティック型ものなどが挙げられる。 具体的に操 作師11は、認証管理師20に機器10の情報を登録す うものであり、例えば、キーボードなどが挙げられる。 尚、操作部11の形状としては、ボタン形状のものや、

8

信号を取得情報管理部13~と出力する。

器認証命令信号が入力された場合は、入力された機器認 路証管理部20との関で路証を行うための賜証命合信号 を検知した場合は、その検知した認証命令信号を取得情 ザの操作により各機器10との間で認証を行うための機 [0055]また、操作師11は、ユーザの操作により 報管理部13~と出力する。更に、操作部11は、ユー 証命合信号を取得情報管理部13~と取得する。

スタ健M)、或いは第二點証情報(認証情報)を複数器 マスタ健M、或いは認証情報を蓄積する。尚、取得情報 [0056] 取得情報潜荷部12は、第一路証情報 (マ **岩段部12には、他の機器10に送信する文字、顔画像など** 1 Cチップなどが挙げられる。具体的に取得情報潜程師 1.2 は、取得情報管理師1.3が通信師1.4から取得した **報する情報潜趙手段であり、例えば、ハードディスク、** の情報データも蓄積することができる。

検知信号が入力された場合は、入力された検知信号に基 [0057] 取得情報管理部13は、機器10の内部動 れる。具体的に取得情報管理部13は、操作部11から ろいた、彼知信号に対応する登録情報を作成する。そし て、登録情報を作成した取得情報管理部13は、その作成 作を制御するものであり、例えば、CPUなどが挙げら した登録情報を要求信号として通信部14〜と出力す

の登録情報を認証管理師20に登録することにより、機 [0058] ここで、登録情報には、例えば、機器10 の名称、機器10を所有するユーザの写真、機器10を 製造販売するメーカ名、機器10のシリアル番号、ユー ザが機器10を購入した年月日、PIN (Personal Ide ntification Number) などが谷げられる。この極路10 器10は、踢監管理部20からマスタ鏈Mを取得すること ができる (群述は後述する)。

[0059] 通信部14から嬰状信号を受信した認証管 号を送信した機器10を認証管理部20の無線ネットワ **一クに属するようにするための登録をし、その登録を行** った機器10にマスタ鏈Mを配布する。取得情報管理部 13は、昭証管理部20から送信されたマスタΦMを通 信部14で受信した場合は、受信したマスタ壁Kを取得 **理部20は、受信した要求信号に払づいて、その要求信** 骨製器積削12に器積する。

[0060]また、操作師11から認証命令信号が入力 された取得情報管理部13は、入力された認証命令信号 を通信部14に送信すると共に、入力された破粉転命令 借号に対応するマスタ健Mを取得情報蓄積即12から取 5。 取得情報管理部13から認証命令信号が入力された 通信部14は、入力された認証命合信号を通信部25に 得し、その取得したマスタ鍵Mを認証部16〜と出力す

13~と出力する。

Ş

広するマスタ健Mが入力された認証部16は、入力され 【0061】取得情報管理部13から認能命令信号に対

校屋2003-101533 たマスク艇Mを用いて、粉缸管理師20にある通信部2 5から送信されたマスタ館Mで呼号化された共通館Kを **石や元し、 その独や元した共通館 K や 取等証金 即 田田 こ** 

取得情報器預節12に器積する。更に、操作師11から 【0062】陽証前16から復号化された共通職Kが入 力された取得情報管理部13は、入力された共通機Kを 入力された機器器組命令信号を器配价模決定価15~と 機器陽配命令信号が入力された取得情報管理部13は、 出力する。

本実施形態では、有効関限判断部15mと、順序部15 [0063] 路証付保決定部15は、他の機器10との間で 通信をするための第二総監情報を確定するものであり、 bと、協定的15cとを作している。

2

ある。具体的に有効関限判断部15nは、取得情報管理 (陽証情報) に含まれる有効期限情報を確認するもので 節13から機器認証命令信号が入力された場合は、取得 竹倒器役割12に潜伐されている共通観Kを取得し、そ の受命した状語館スパボムへと、その状語館スパにせた 期)を判断し、その有効期限を判断したことを示す判断 [0064] 有効期限判断部15mは、第二路監情報 ている行参規限信仰から共通職人の行参規限(特)時 得号を取得得報管理部13と、現所部156とへ出力す 2

その並び換えた結果を示す並び換え結果情号を遵定部15 る。具体的に順序部156は、有効関限判断部15aか 揺るいた、取得情報謝預節12に謝留されたいる複数を 在多期限位置に基めいた、その在後が限位的に対応する 複数の第二器証情報を所定の順番に並び換えるものであ [0065] 順序部156は、第二路監督報に合まれる ら判所信号が入力された場合は、入力された判所信号に る路証情報を、例えば有効期限が近い順番に並び換え、 c へと川力する。

8

[0066] 遊定部15cは、取得情報期位部12に複 から、政第二路監督和に会まれる有効期限情報に基づい 定する確定手段である。具体的に確定部15cは、順序 その判断した結果を使用判断借分として取得情報管理部 数書位されている有効期限情報を含む第二路配情報の中 て、版有効期限情報に対応する一つの第二認能情報を遵 第155から並び換え結果信号が入力された場合は、入 力された並び換え結果信号に括ろいて、並び換えられた 路証价組のうち、どの認証情報を使用するかを判断し、

[0067] 例えば、並び換え結果信号信号が入力され て、有効期限順に並び換えられた認証情報のうち、有効 期限の終了時期が長い認証情報を、各機器10との間の **た遊定部15cは、入力された並び換え結果信号に基づい** 路話に使用するなどと判断する。

[0068] また、母定部15は、他の複器10 b に 打する 枚数の第二點類情報(共通職民)に会まれる機関子を収

-1-

るための検知信号を検知した場合は、その検知した検知

20

**得し、その取得した職別子と、機器10gに有する複数** 情報のうち、数額別子に対応する値配有効期限情報に基 の第二路監信権に含まれる韓別子との間で共通する韓別 子を抽出して、その抽出した模別子に対応する第二結論 報を確定する第一箇定手段でもある。

た場合は、操作部11は、その検知した機器認証命令信 [0069] 具体的には、先ず、操作部11 (機器10 4にある操作部11)が、ユーザの操作により機器10 bとの間で器証を行うための機器器証命合信号を検知し りを取得情報管理部13に出力する。

01

号が認証情報に含まれる職別子に基づいて認証情報を遵 【0070】操作師11から機器器距命合信号が入力さ れた取得情報管理部13は、入力された機器認証命令信 定すべき信号であると判断した場合は、その入力された 機器器監命令信号を過定部15cに出力する。尚、取得 情報管理部13は、入力された機器認証命令信号が認証 情報に含まれる有効期限情報に張るいて認能情報を選定 すべき信号であると判断した場合は、その入力された機 器器監命令信号を上記有効期限判断部15 a に出力す

20

[0071] 取得情報管理部13から機器認証命令倡号 信号に基づいて、例えば、機器器組命合信号に対応する が入力された強定部15cは、入力された機器認証命令 賜証僣棋の識別子(n-3、n-2、n-1、n)を取得情報署 **업部12から取得し、その取得した観別子 (n-3、n-2、** n-1, n) を通信部14~と出力する。

(n-3, n-2, n-1, n)を機器10bの通信部14~と送 **信する。一方、機器10bは、上記手順と同様に、例え** ば、機器105の取得情報搭積部12に搭積されている 【0072】 遊定部15cから臨別子 (n-3, n-2, n-1、n)が入力された通信部14は、入力された職別子 数別子 (n-3, n-2, n-1) を、競別子 (n-3, n-2, n-1、n)を送信した機器10mに送信する。

別子 (n-3、n-2、n-1、n)を取得情報器預節12から 【0073】機器10aの通信部14は、機器10bから **韓別子 (n-3、n-2、n-1) を受信した場合は、受信した** 力された強定部15cは、自機が使用する認能情報の職 そして、通信郎14から模別子 (n-3, n-2, n-1) が入 と、通信部14から入力された戦別子 (n-3、n-2、n-**数別子 (n−3、n−2、n−1)を強定部15○へと出力する。** 取符し、その収符した観別子 (n-3, n-2, n-1, n) とを比較する。

【0075】 観別子n-1を選定した選定部15cは、選 る。また、この磁別子n-1の遊定は、機器10bにある は、例えば、その一致している額別子 (n-3, n-2, n-1) のうち、有効期限下が一番及い類別子n-1を強定す 3, n-2, n-1) は、一致しているので、選定部15c 【0074】 岡者の臨別子を比較すると、臨別子 (n-使用部14cでも、上記同様の手順により行われる。

間する情報データを暗号化し、通信部14は、その共通 応した観別子 n−1に対応する共通観K n−1を、取得情報 搭位部12から取得し、その取得した共通鍵Kn-1を認 **院部16~と出力する。そして、違定部15cから観別子** は、入力された共通離Kn-1を用いて、機器10bに送 職Kn−1で暗号化した情報データを機器10bへと送信 n-1に対応する共通鍵Kn-1が入力された認証部16

い。これにより、機器は、第二認証情報の有効期限を管 【0076】尚、遠定部15cは、秘密情報生成部22(生 成手段)で所定の周期毎に生成された第二陽監情報を複 数取得し、その複数取得した第二點監情報の個数が所定 の個数を超えたときは、取得した複数ある第二認証情報 のうちのいずれかを削除する第三選定手段であってもよ 理する必要がなくなり、更に、有効期限を管理するため の時間管理部(図示せず)を設ける必要がない。

【0077】 認証部16は、認証管理部20から予め取 部26との間で通信をするための認証を行う第二認証率 段である。具体的に認証部16で行う認証は、図3に示 すように、無椴ネットワークプロトコルのOSIを用い 機器10bとの間で共通の共通艦Kは、先ず、認能管理 をマスタ鍵Mで暗号化する。尚、共通鏈Kは、秘密情報 した機器10g(通信部14で取得)は、機器10gに 得してある第一認証情報(マスタ鍵M)を用いて、認証 て説明することができる。同図によれば、機器10aと 部20にあるOSIのアプリケーション函か、共通**顧K** [0078] マスタ鍵Mで暗号化された共通鍵Kを取得 マスタ鍵Mで暗号化された共通鍵Kを、取得情報管理部 生成部22で生成されるものである (詳述は後述する)。 ある駱駐部16にある081のアプリケーション扇で、

通線Kを復号化した認証部16は、復号化した共通鍵K 1 3から入力されたマスタ母Mを用いて復号化する。共 を取得情報管理部13~と出力し、認証部16から共通 鍵Kが入力された取得情報管理部13は、入力された共 通銭Kを取得情報蓄積部12に蓄積する。

通信部14は、認証管理部20から要求信号に対応する マスタ壁Mを受信した場合は、受信したマスタ壁Mを取

得情報管理部13へと出力する。

第二點指指数 (共通鍵K)を用いて、他の機器10 b との [0079]また、認証部16は、通信部14で受信した ら機器10aと機器10bとの間で共通の共通鍵Kを取 **鈴する。共通離Kを取得した認覧部16は、OSIの庁** る。具体的に認証部16は、機器10aと機器10bと の間で通信をするための認証を行う場合は、適定部15か (例えば、文字データ、画像データなど) を、取得した 間で通信をするための認証を行う第二認証手段でもあ **ータリンク局で、機器10bに送信したい情報データ** は通難Kを用いて暗号化する。

16は、共通戯Kで暗号化した情報ゲータを、OSIの [0080] 信報データを共通額Kで語号化した認証部 0 a から共通鍵K で暗号化された情報データを取得した データリンク層を通じて通信部14から送信する。機器1 機器10bの認証部26は、共通鍵Kで暗号化された情報デ

**ータを、機器10bが予め有している共通鏈Kを用いて** 

[0081] これにより、共通鉄Kは、路筒管単部20 で、共通鏈Kを有する機器10mは、共通鏈Kを有する **街の籔路10bとの匠では、位勢ゲークを共通顧Kが時** に登録した全ての機器10a (10b) へと配布されるの **号化して送信することができるので、所定の怙殻データ** が外部の者に強視されることがない。

て認証管理師20にある通信師25から第二路監情報を 受信する第二通信手段である。通信部14は、例えば、BI 02. 11、或いはIrDAによる通信方式を用いた通信機 【0082】通信部14は、陽証部16の陽距に基づい uetoothによる通信方式を用いた通信機器、1 EEEE8 器などが挙げられる。

3から認証命令信号が入力された場合は、入力された認 は、その受信したマスタ鏈Mで暗号化された陽監情報を 証命令債号を認証管理師20にある通信部25に送信す る。通信部14は、通信部25から路距命令信号に対応 するシスタ鍵Mで暗号化された共通鍵Kを受信した場合 [0083] 具体的に通信部14は、取得情報管理部1 認証部16へと出力する。

から要求借号が入力された場合は、入力された要求信号 壁Mで暗号化された認証情報を、取得情報管理部13か ら入力されたマスタ壁Mを用いて復号化し、その復号化 された認証情報を取得情報管理部13~と出力し、復号 【0084】通信部14からマスタ健Mで暗号化された 認証情報が入力された認証部16は、入力されたマスタ [0085]また、通信即14は、取得情報管理部13 化された認証情報が入力された取得情報管理部13は、 入力された認証情報を取得情報蓄積部12に書積する。 を認証管理部20にある通信部25に送信する。更に、 [0086] 通信部14からマスタ鍵Mが入力された取 得情報管理部13は、人力されたマスタ健Mを取得情報 蓄積部12に蓄積する。その後、操作部11から機器器 証命令倡号が入力された取得情報管理部13は、入力さ れた機器認証命令倡号に基づいて、マスタ雙Mを取得情 報書預部12から取得し、その取得したマスク健Mを認 証部16~と出力する。

【0087】また、通信部14は、路証部16の路証に 払ろいて、他の破路10との回の通信を行う第二通信手 段でもある。具体的に通信部14は、認証部16から共通 力された共通線Kで昨号化された信報データを他の機器 **雌Kで暗号化された情報データが入力された場合は、入** 106に送信する。

は、操作部21と、秘密情報生成部22と、秘密情報器 [0088] 前記認証管理部20は、所定の秘密情報を 管理するものであり、図1に示すように、本実施形倣で

**参照2003-101533** 

9

[0089] 秘密情報生成部22は、陽監管明部20と機 預部23と、秘密情報管理師24と、通信部25、186証制26 **かかなしたいる。毛、薬化師21は鞍作師11と左節数** 器10ヵとの凹で通信を行うための第一路証情報(マスタ 陸M)と、機器10nと他の機器10bとの川で通信を行う **れめの初川総盟社会(共通額K) わからなる総配信金や** 隋が同僚であるので、敬作師21の説明は省略する。 生成する生成年段である。

5マスタ健Mと登録情報とが入力された秘密情報管理部 健Mを通信部25~と出力する。秘密情報生成部21か 24は、入力されたマスク壁Mと登録情報とを秘密情報器 りに基づいて、その要求信号に対応するマスク健Mを生 生成したマスタ健Mと、坂水信号(恐婦信仰)とを秘密 [0090] 具体的に秘密情報生成開21は、通信開2 5から要求信号が入力された場合は、入力された要求信 情報管理部24~と出力すると共に、その生成したマスタ 成する。マスク壁Mを生成した秘密情報生成部21は、 資商23に潜稿する。 9

払ろいて陽配信権を逐次生成し、その生成した陽配信権 [0091]尚、陽龍情像(共通難K)は、定期的に生 成されるものである。具体的には、秘密情報生成師22が CPU (図示セす) で管理されている時間信報 (時刻) に を秘密情報器積開23に器積する。 20

入力された通信部25は、入力されたマスク健Mを、要 [0092] また、秘密情報生成師22からマスタ壁Mが 女信号を送信した機器10~と送信する。通信信25か らマスタ醚Mを受信した適信部14は、取得したマスタ マスタ健Mが入力された取得情報管理部13は、入力さ タ壁Mが秘密情報器積御23に器積されたことを意味す **陳Mを収得情報管理部13~と出力し、通信部14から** 怒監管理部20~の登録とは、登録情報に対応するマス れたマスク壁Mを取得情報器預問12に器積する。尚、

め登録(上記手順を奪服のこと)されたものであり、認 に、機器10a及び機器10bは、認証管理開20に予 [0093] 図4は、認証管理師20が、秘密情報生成 部22で生成された秘密情報を機器10a及び機器10b 証管理師20から送信されたマスタ壁M n 又はマスタ健 Mb が保存化された共通額Kを、認証を担信20から股 し、その復步化した共通館Kを機器10m又は機器10 に配布する様子を示したものである。同図に示すよう 得したマスタ鏈Ma及びマスタ鏈Mbを川いて復号化

[0094] また、機器10cは、陽監管照開20に登 **染されていないので、板端10g及び板路10bとの同** では粉缸を行うことができない。これにより、機器10 n及び機器10bは、機器10n及び機器10bとの間 **で共通の共通額<br />
なが右しているのか、共通額<br />
を繋ぐ** した無数ネットワークを形成することができる。 bとの間の総額に用いることができる。

[0095] 図5に示すように、機器10cが、機器1

20

Ξ

り、共通観Kを復号化した機器10cは、同図に示すよ うに、機器10cに有する共通線Kを用いて、共通機K を有する機器10m及び機器10bの間で形成される無 マスタ鍵M c を要求する要求信号を認証管理部20に送 **借した場合は、認証管理部20は、その受信した要求信** [0096] 認証管理師20からマスタ壁Mcを受信し り行された共通額Kを認能管理部20から数値し、その 受信したマスタ鍵Mcで暗号化された共通鍵Kを、前に た機器10cは、図6に示すように、マスタ鍵M c で暗 取得したマスク壁Mcを用いて復号化する。これによ 0 a 及び10 b に共通する共通額Kを取得するために 号に対応するマスタ壁M cを機器10 cに送信する。

uetoothによる通信方式を用いている場合は、Bluetooth の種類を散定することができる。例えば、秘密情報生成 による通信方式に対応したマスタ鍵Ma1及びマスタ鍵M 機器10に用いられている通信方式に応じてマスタ壁M 第21は、同図中のBT機器10n及び機器10bがB 【0097】秘密情報生成部22は、図7に示すように、 82を生成することができる。 [0098] 認能管理部20からマスタ壁M81又はマス 夕壁M82を取得したBT機器10g及び10bは、認証 式を用いた機器10間で認証を行うキー)を、前に取得 **管理部20から送信されたマスタ醚MBI 又はマスタ键M** その復号化した共通館KIを用いてBT機器10a及びB したマスタ壁MB1及びマスタ艇MB1を用いて復号化し、 1.2 で暗号化された共通額K1 (Bluetoothによる通信力 1.機器106の間で認能をする。

2. 11機器10c~10cが802. 11による通信 [0099] 一方、秘密情報生成部22は、同図中の80 方式を用いている場合は、802.11による通信方式 用いて復号化し、その復号化した共通韓ス2を用いて8 を取得した802. 11機器10c~10cは、認証管 職K2を受信し、前に取得したマスタ鍵M81~M83を に対応したマスタ鍵MoI~MB3を生成することができ る。 認証管理部20からそれぞれマスタ雄Ma1~M 8 3 理部20からマスタ鍵Mn1~M83で時号化された共通 02. 11機器10c~10cとの間で認証をする。

10で採用されている通信方式に応じてマスタ壁Mを生 成することができるので、各機器10は、自機で採用さ れている通信方式に応じたマスク鍵Mを取得することが 【0100】これにより、秘密情報生成部21は、機器 でき、更に、自機が採用している通信方式と同一である 他の機器10との間で無線ネットワークを形成すること

とができる。更に、CPUスペックが小さく、リアルタ [0101] また、陽証管理部20は、上記より1EE E802.11、Bluetooth、HiperLAN2などの通信方式 が異なる機器10毎にマスタ雛Mの傾筋を換えることに よって、通信方式が異なる複数の機器10を管理するこ

イムクロックを持たない機器10は、各機器10間で共 によって各機路10回との回の無袋ネットワークを簡単 38監管理部20から送信されるマスタ壁Mを用いること 通の認証情報などを生成することなどが困難であるが、 に形成することができる。

た要求信号を秘密情報生成部22~と出力する。尚、認証 る。更に、通信部25から認証命令信号が入力された秘 密閉報管理部24は、入力された認証情報命令倡号に基 【0102】秘密情報管理部24は、認証管理部20の内 部動作を制御するものである。具体的に通信部25から 要求倡号が入力された秘密情報管理部24は、入力され **管理部20への登録とは、登録情報に対応するマスタ離** [0103]また、秘密情報管理部24は、秘密情報生成 吹いは認証情報が入力された場合は、入力されたマスタ ろいて、その認証命合倡号に対応するマスタ鍵Mと共通 健Kとを秘密情報潜程第23から取得し、その取得した 雕M、踢脏情報、登錄情報を秘密情報蓄積部2312搭積す Mが秘密情報管理部23に蓄積されたことを意味する。 第22から要求信号に対応する生成されたマスク鍵M、 マスタ鍵Mと共通鍵Kとを認覧部26へと出力する。

模ネットワークに属することができる。

【0104】秘密情報書積部23は、秘密情報生成部22で るものであり、例えば、ハードディスクなどが挙げられ る。具体的に秘密情報蓄積部23は、秘密情報管理部24か は、入力されたマスタ壁M、認証情報、登録情報を蓄積 生成された秘密情報 (マスタ壁M、路証情報) を書積す らマスタ壁M、認証情報、登録情報が入力された場合

[0105]通信部25は、認証部26の認証に基めいた策 二點胚情報(賜証情報)を送信する第一通信手段であ

夕健Mが入力された通信部25は、入力されたマスク鍵 器、IrDAによる通信方式を用いた通信機器などが挙げら 合倡号)を受倡した通倡部25は、受倡した要求信号(或 また、秘密情報管理師24から要求倡号に対応するマス れる。具体的に通信部14から要求信号(或いは陽監命 り、例えは、Bluetoothによる通信方式を用いた通信機 いは認証命合倡号)を秘密情報管理部24へと出力する。 Mを、要求信号を送信した通信部14に送信する。

[0106] 認証部26は、秘密情報生成部22で生成され マスタ壁Mで暗号化された認証情報が入力された通信部 25は、入力されたマスク壁Mで暗号化された認証情報 を機器10に送信する。尚、認証部26で行われている内 た第一器証情報を用いて、機器10との間で通信をする ための認証を行う第一認証手段である。具体的に認証部 26は、秘密情報管理部24から認証命令信号に対応するマ スタ壁Mと認証情報とが入力された場合は、入力された 認証情報をマスタ壁Mで暗号化し、そのマスタ壁Mで暗 部処理は、上述した路距部16と同様の内部処理が行われ **号化した認証情報を通信部26に出力し、認証部26から** 

【0107】 (機器認証管理システムを用いた機器認証

20

(12)

同図中における丸く囲まれている部分は、機器10の状 随を意味しており、また四角で囲まれている部分は、処 ができる。図8は、本実施形像に係る機器路配管理方法 管理方法)上記構成を有する機器認監管理システムによ る機器賜証管理方法は、以下の手順により災施すること の全体のフロー(状態選移)を示したものである。尚、 単を意味している。

**得した機器10が、取得した認能情報を用いて他の機器** の認証情報を管理する認証管理師20から認証情報を取 [0109] 先ず、機器10が路証管理部20に登録さ 管理部20に登録することを行う(S1、S2)。機器 器は、認証管理部20からマスタ壁Mを取得することが できる (53)。そして、認証管理部20からマスタ値 Mで暗号化した共通館Kを取得した機器10は、その取 S3で取得したマスタ壁Mを用いて共通壁Kへと復身化 [0108] 同國に示すように、認証管理方法は、所定 **れていない場合は、機器10は、自機の登録情報を認証** 10を認証管理部20に登録すると、その登録された機 得したマスタ健Mで呼号化された共通観Kを、ステップ 10との間で通信をするための認証を行うものである。 して共通鍵Kを取得する (S5~S9)。

[0110] その後、機器10は、復与化した共通艦K を用いて、他の機器10との間で認証を行い、 認証が改 いる登録情報に対応するマスク鍵Mを削除することによ り行う (S13~S15)。 上配に示す、機器路配方法 を構成する各手順の群遊は、以下の手順により説明する (S10~S12)。 尚、認証管理部20で登録された 機器10を削除するのは、認証管理部20で蓄積されて 功した他の機器10との間で情報データを送受信する

スタ観Mと共通観Kとを取得する方法

ことができる。

図9は、機器10が認証管理部20からマスタ鍵Mと共 **通録Kとを取得する手順を示したものである。 阿図に示** すように、先ず、機器10が認証管理部20に対して登 験情報を送信するステップを行う (S101)。 具体的 には、取得情報管理部13が、操作部11から検知信号 が入力された場合は、入力された検知信号に基づいて、 その検知信号に対応する登録情報を作成する。 [0112] そして、機器10がマスタ壁Mを取得する ためには、操作部11及び操作部21の河省においてユ ーザの操作 (この操作には陽監情報の入力、例えばPI 3 は操作部11から検知信号が入力された場合、要求信 号(これには登録情報は含まれない)を通信部を経由し Nの入力が含まれる)が必要である。取得情報管理部1 て陽監管理節20に送信する。

いる場合は除く。操作部21に検出信号がある前に上記 [0113]一方、認証管理部20は操作部21に検出 信号があった場合、機器10から上配要求信号が送仰さ れるまで待機する。ただし上配要求信号を既に受信して

以水信号を受信した場合は、認能管理部20は機器10 から、上配要米信号が送信されるまで特徴する。

校宝2003-101533

与があった後で、錫紅管里師20は錫紅手順開始要求を 機器10に送信し、認能管理部20と機器10の間の認 路10から熨米信号を受信し、かつ操作信21に検川信 [0114] (上記段格に記載のいずれかの方法で) 証手順を開始する。

[0115]この陽話手間の具体的な内容はここでは近 が入力したPINと比較する、方池がある。又は、機器 行うこともできる。更に、(後述する)マスク鍵Mの道 10と協能管理師20の間でDiffie-Hellman鍵交換等の INとその他登録情報の送信はこの健により昨步化して 殺しないが、例えば機器10が操作師11にユーザの入 カしたPINとその他登録情報を認証管理師20に送信 し、酩藍管理師20はこのPINを操作師21にユーザ 方法により (一時的な) 雌の生成を最初に行い、上紀P 信も、ここで生成した観を使って行うことができる。こ の難は登録手順 (図9の手順) が完了すると廃棄され

ば、機器10のPINは製造時に描り当てられた固定の とができる。この場合以来信号は機器10ではなく、場 の磁伯を図状することにしたが、別の倒としては、どち 値にし、これを操作部21に入力することにより行うこ [0116] 賜龍平胤が成功した場合のみ (PINが一 い)、以下のマスク艇Mの生成等が行われる。尚、ここ では原因とした核作師 | 1と核作師 3 1の過力でユーシ らか一方の操作を省略する方法であってもよい。例え 致しない等の理由で失敗した場合は基録を続行しな 部件単価20が機器10に向けて送信する。

20

[0111] Xいで、8粒管型間20が、機器10との 行う (S102)。 具体的には、通信師14から奥米信 りを受信した適信師25は、受信した要求信りを秘密情 **衛管理師24~と出力する。そして、通信師25から要** 東信号が入力された秘密情報管理部24は、入力された たマスタ壁Mを散当する機器10に送信するステップを 間で認証を行うためのマスタ壁Mを生成し、その生成し 要求信号を秘密情報生成師22~と出力する。 30

[0118] その後、協僚情報管理師24から要求信号 が入力された秘密情報生成師22は、入力された要求信号 する。マスク壁Mを生成した協密情報生成師21は、生 成したマスタ鍵Mを秘密情報管理師24へと川力すると共 する。秘密情報生成師22からマスク壁Mが入力された秘 に基ろいた、その要求信号に対応するマスク観Mを生成 に、その生成したマスタ壁Mのみを通信師25〜と川力 を秘密情報器積削23~と器積する。尚、路監管期間20 が機器10を登録するとは、登録情報に対応するマスタ 【0119】そして、秘密情報生成師22からマスタ離 密情報管理師24は、入力されたマスク鍵Mと登録情報と 題Mを秘密情報器位置23に器位することを意味する。 \$

Mが入力された通信部25は、入力されたマスク键M

を、夏水信号を送信した通信部14へと送信する。その は、受借したマスタ健Mを取得情報管理部13~と出力 し、通信部14からマスタ鍵Mが入力された取得情報管 理部13は、人力されたマスタ鍵Mを取得情報書程部1 後、通信師25からマスク壁Mを受信した通信師14

的には、取得情報管理部13は、認能命令信号を通信部 る可能性もあるので、このタイミング以外でもときどき [0120] 点、認能管理部20は定期的に共通職Kを 生成するので、その直後に認能管理部20から転送開始 Oに共通額Kの信送を行ったかどうか、というリストの 哲理を省くことが可信となる。更に、共通題Kに有効期 限情報が設定されているとき、機器10が自身の持つ共 通難Kの有効期限が切れるおそれがあると判断した場合 【0122】次いで、機器10が、器監管理部20から 共通難Kを取得するステップを行う(S103)。 具体 14に送信すると共に、マスタ壁Mを取得情報蓄積部1 2から取得し、その取得したマスタ鍵Mを認証第16〜 の収求を行う。このときに通信可能でない機器10があ [0121] これにより認証管理部20は、どの機器1 と出力する。取得情報管理部13から認証命令信号が入 カされた通信部14は、入力された認能命令信号を通信 にも、機器10の倒から伝送用始の要求をしてもよい。 (例えば、症期的に) 伝送開始の要求を行ってもよい。 部25に送信する。

監信報命合信号に基づいて、その認能命令信号に対応す るマスタ壁Mと認証情報とを秘密情報器積部23から取 【0123】その後、通信部14から路監命合信号を受 **聞した通信部25は、受信した認能命令信号を秘密情報管 理部24~と出力する。そして、通信部25から認監命令** 倡号が入力された秘密情報管理部24は、入力された認 得し、その取得したマスタ壁Mと認証情報とを認証部2 6~と出力する。

Mで呼号化された認証情報を機器10に送信し、通信部 【0124】そして、秘密情報管理部24から認証命合信 **りに対応するマスク健Mと認証情似とが入力された認証** し、そのマスタ艇Mで暗号化した認証情報を通信部25 に出力し、認証部26からマスク壁Mで暗号化された認 証情報が入力された通信部25は、入力されたマスク鍵 1.4 は、通信部2.5から送信されたマスタ鍵Mで暗号化 部26は、入力された認証情報をマスタ鍵Mで暗号化 された認証情報を受信する。

40

[0125] 次いで、取得情報管理部13から認証命令 入力されたマスタ母Mを用いて、通信部14で受信した マスタ麒Mで暗号化された共通鍵Kを復号化し、その復 そして、認証部16から復号化された共通録Kが入力さ れた取得情報管理部13は、入力された共通館Kを取得 り化した共通庫Kを取得情報管理部13へと出力する。 信号に対応するマスタ鍵Mが入力された認証部16は、 間報書位即12に著位する。

【0126】 そした、 馥略10が、 共通算K か形成がれ **共通鍵Kを各機器10周の認証に用いることにより、共 通難Kで形成された無線ネットワークに参加することが** た無数ネットワークに参加する場合は、上記復号化した 연출점 (S 1 0 4) 。

[0127] 尚、認証管理部20に登録してある機器1 ず、機器10が、認証管理部20に対して、登録を削除 0の登録を削除する方法は、図10に示すように、先

するための削除情報を送信するステップを行う (S20 1)。ここで、機器10の登録を削除するとは、秘密情 粗器損部23に蓄積されている整線情報に対応するマスタ 健Mを削除することを意味する。

0

により認証管理部20に登録してある機器10の登録を 削除するための信号を検知した場合は、認証管理部20 に登録してある機器10の登録を削除するための検知信 号を、取得情報管理部13に出力する。そして、操作部 入力された検知信号に基ろいて、認証管理部20に登録 してある機器10の登録を削除するための登録削除信号 出力する。その後、取得情報管理部13から登録削除借 号が入力された通信部14は、入力された登録削除信号 【0128】具体的には、操作部11が、ユーザの操作 を生成し、その生成した登録削除倡号を通倡部14〜と 11から検知信号が入力された取得情報管理部13は、 を該当する通信部25に送信する。

20

【0129】その後、秘密情報管理部24は、マスタ壁 は、通信部14から登録削除借号を受借した通信部25 は、受信した登録削除信号を秘密情報管理部24~と出力 する。更に、通信部25から登録削除信号が入力された 秘密情報管理部24は、入力された登録削除信号に基づい Mを削除するステップを行う (S202)。 具体的に

[0130]次いで、認証管理部20は、秘密情報管理 ので、登録削除信号を送信した機器10に共通鏈Kを送 て、登録削除信号に対応するマスク壁Mを秘密情報蓄積 部23から削除する。尚、マスタ壁Mは、認証管理部2 第22が機器10に対応するマスタ艇Mを削除している 0にある操作部21を介して削除することもできる。

は、認証管理部20からマスタ壁Mで呼号化された新た な共通難K、を取得することができないので、予め取得 してある共通難Kの有効期限が切れたと何時に、共通難 K. ひ形成かれた無袋ネットワークに成かめいわがため 伯しないようにする (S203)。 その後、機器10

【0131】即ち、機器10は、認能管理部20から共 通難Kを取得したとしても、その取得した共通難Kに右 **効期限が設定されていれば、その共通額Kの有効期限が** 凹れたア国母に、共通難下で形成された無数ネットワー クに届することができなくなる。

[0132] (2)機器10が、認証管理部20から取 **認証情報に含まれる有効期限情報(共通観K1~K3に 沿した複数ある認能情報(共通鍵KI~K3)のうち、** 

€

45万十る有効期限情報に1~13)に基づいた、他の機 器との間で器配する際に使用する一つの共通館を選定す

したものである。同図に示すように、機器10cは、取 特情報器預部12にある取得情報テーブルに複数の認証 ている複数の認証情報のうち、認証情報に含まれる有効 際に使用する一つの共通観を選定する手順を概念的に示 図11は、機器10が、取得情報器積飾12に書積され **基限計画に基ムにた、他の複略10との画が緊閉を行う** 位数を指位している。

位されている認証情報のうち、有効期限下3が及い共通 難K3を遺定する方法がある。尚、TnとKnにある旅 え文字nは、1、2、3・・・・の数字を意味するもの 【0133】機器10cが、機器10nXは機器10b かを過定する方法は、例えば、取得情報蓄積部12に書

1に対応する有効期限T3~T1 (この順番は有効期限 め、機器10cにある強定部15cは、取得情報器傾部 [0134] 取得情報書積部12に書積されている認証 **曽根は、回図に示すように、認能情報の識別子n3~n** が扱い順番)と共通離K3~KIとを在している。このた 1.2に潜位されている共通盤K.1~K.3のうち、有効型 有効期限が一番長いK3を勘定することになる。この共 限が一番長い共通鍵を選定すると設定している場合は、 通難の避定方法は、具体的には以下の通りである。

を操作させることにより、各機器10との間で路証を行 部11は、その検知した機器認証命令信号を取得情報管 理部13~と出力する。そして、操作部11から機路路 証命令倡号が入力された取得情報管理部13は、入力さ れた機器器監命合信号を有効期限判断部15 n ~と出力 [0135] 先ず、操作師11が、ユーザに操作師11 うための機器認証命令信号を検知した場合は、その操作

[0136] その後、取得情報管理部13から機器器証 K3) を取谷し、その取谷した認覧信仰に基めいた、そ T3から共通館K1~K3の行効期限を判断し、その行 効期限を判断したことを示す判断信号を取得情報管理部 命令信号が入力された有効期限判断部15gは、取得情 **敷潜街節12に潜街されている駿監庁僚(共通艦K1~** の共通数K 1~K 3 に合まれている

方数型

原存を

「1~ 13と、順序部15bとへ出力する。

払ろいて、取得債報群位部12に潜債されている複数あ その並び換えた結果を示す並び換え結果倡号を遊定即15 【O137】そした、在悠辺限判歴部15aから対歴部 号が入力された順序部156は、入力された判断信号に る路証情報を、例えば有効期限が近い順番に並び換え、

身が入力された強定部15cは、入力された並び換え結果 【0138】次いで、順序曲15bから並び換え構果間

信号に基づいて、並び後えられた陽監信仰のうち、有効 **芦展が一般及い路覧位格(共通観K3)を使用すると地** 断し、その使用すると判断した陽監情徴を陽脈師16〜

校屋2003-101533

独に会まれる観別字に基ムされ、他の複類回を用いる語 カされた昭和部16は、人力された共通権区3に基づい 1参照)。尚、上紀年順は、複数の総証併復に含まれる **冶多逆室苔色に揺んいた、蚕路10m(10p)を川い** る陽証情報を遵定(他の機器10ヵ及び機器10ヵは、41 数の陽龍情報)したが、後述する手順(3)は、陽龍情 【O 1 3 9】 そした、随近郎 1 5 cから共通職K 3 が入 て、破路10g及複路105との間の路底を行う(図1 (3) は、国機器に行する認能情報の数が複数でも同者 証信報を選定することもできる。また、後述する事順 に共通する陽配情報を確定することができる。

[0140] (3) 機器10nが、BB配信仰に含まれる 報別子に 据るい ケ色の 観路 10 b v の 回 v 川 v の 場所 位 報を選定し、その選定した認証情報を用いて他の機器1 0 b との国で通信を行う方法

路10ヵに対した、使川することが可能な共通額大の観 図12は、機器10ヵが他の機器105との間で共通館 別子nを送信するステップを行う(S301)。 具体的 ある。同図に示すように、先ず、機器10ヵが、他の機 ための機器認証命令信号を検知した場合は、操作師11 Kを用いて情報ゲータを込及信する方法を示したもので には、先ず、操作師11 (機器10にある操作師11) が、ユーザの核作により機器10bとの凹で路話を行う は、その検知した機器陽配命合信号を取得情報管理師1

14~と出力する。その後、取得情報管理部13から概 群位師12から取得し、その取得した職別子nを通信師 【0141】そつた、核作節11かの機路観覧命令行ぶ が入力された取得情報管理部13は、入力された機器器 人力された機器影話命令信号に基ろいて、機器影話命令 信与に対応する観別子』(認証情報の一部)を収得情報 語命合信号を確定部15ckHカし、収得信仰管理部1 別子nが入力された通信部14は、入力された微別子n 3から機器陽距命令信号が入力された強定部15cは、 を被殺105の通信部へと送信する。 3~と出力する。 2

(機器105が所有している共通臨K5の観別字) とを る共通観Kを用いて機器105に送信する情報ゲータを 2)と同様に、機器105の取得情報器損削125に器 機器10mは、自機の取得特性機能位置1.2に期債されて 比較し、国名が一致したいる場合は、観測子=に対応す 積されている観別子nbを、臨別子nを送信した機器1 Onに送信するステップを行う (S302)。 その後、 [0142] 一方、機器10bは、上記年順 (S30 いる種別子nと、機器10bから受信した観別子nb 昨号化するステップを行う (S303)。 \$

[0143] 以体的には、機器10nにある適价部14

8

aが、複路10bから鏡別子nbを原料し、その原料した鏡別子nbを建定部15c~と出力する。そして、通信部14aから鏡別子nbが入力された使用部10cは、自動が使用する共通難K(使用する共通難Kを確定する方法は、上記(2)を参照のこと)の鏡別子nを使得相報者信託12から吸引し、その原料した鏡別子nとを存得に関から入力された鏡別子nbとを比較し、その両者を比較した結果、両者が一致していれば、鏡別子nに対応する共通難Kを認能部16へと出力する。

[0144] 尚、勤定師15cが、職部10aと機器10bの職別1を比較した結果、複数の協別子を比較し、その両者を比較した結果、複数の職別子(n~n-2)に対応する認証情報のうち、その疑別子(n~n-2)に対応する認証情報のうち、その疑別子(n~n-2)に対応する認証情報のうち、その職別子(n~n-2)に対応する認証情報のうち、その職別子(n~n-2)に対応する認証情報に振りいて、例えば有効原限が及い機別子のに対応する認証情報Knを適定する(図13参照)。

9

【0145】その後、遠定部15でから識別子市に対応する共通離Kが入力された認証部16は、入力された共通 盤Kを用いて、機器10トに送信する情報データを職器1亿し、その共通離Kで晴号化された情報データを機器10トと送信する(S303)。機器10市から共通難 Kで晴号化された情報データを機器10トの路 経際は、受信した共通館Kで晴号化された情報データを、自機が行する疑別子市トに対応する共通鍵Kト(機器10市の共通键Kと同じ)を用いて復写化(S304)し、機器10市から送信された情報データを取得す

(0146)これにより、機器10mは、機器10mにある情報データを、共通鍵化を用いて時分化して機器10bに送信することができるので、緊痛管理師20を介存させなくても情報データを送信することができる。
(0147]前、図13元字まように、機器10m~10mが数数の共通性n~kn~2を行している場合は、土地と同級の手類により、例えば、機器10m~10cに指導データを送信することができる。機器10mが他の機器10bを送信するように関係データを送信することができる。機器10mが他の機器10bを送信する方にもがの機器10bを送信する方にある。機器10mが他の機器10bを送信する方によいて両機器90m(10b)に行する認定所において両機器90m(10b)に行する認定的

**【0148】(4) 複数10a及び10bが、ある時点において函数310a(10b)に打している認能情報が10a(10b)に打している認能情報が図ーでない場合の過度力法** 

(3)の方法では、ある時点において各機器10に有している共通離水が同一である場合の通信方法について観明したが、(4)では、ある時点において各機器10に有している共通離水が同一でない場合の通信方法について数別する。図14は、ある時点において、機器10a

及び機器10bに有する共通鍵Kが異なる場合の通信方法の概要を示したものである。

[0149] 同図に示すように、ある時点において機器10mを機器10mにある非面離Kの種類が異なると、機器10mと機器10mとは、両者の間で情報データを送受信することができなくなる。このため、機器10m及び機器10bに、以下の平衡による方法で機器10mと機器10mの間で指触データの送受信を行う。

[0150] 同図に示すように、認証管理師20では、 共通難をKn-3、Kn-2、Kn-1、Knの順序で生成し、樹 路10a及び機器10bでは、認証管理師20で生成されて合大兵道整Kn-3、Kn-2、Kn-1、Knを吸得し、その 原行した各共通難Kn-3、Kn-2、Kn-1、Knを吸得し、その 原行した各共通難Kn-3、Kn-2、Kn-1、Knを吸得し、その 原行した各共通難を取る材が報音位師12に若似する。 在は、現なものとする(同図を照)。また、同図に示す 取料相表一プルとは、取料相違数位部12に若似されている場では、 取れている多配情報(整別子n、イ外期限工、共通鍵Kな でいる認証情報(整別子n、イ外期限工、共通鍵Kな とも等例の概形で示したものである(呼系列は上の 段から始まるものとする)(「販売情報テープル」は、 以下同に意味を有するものとする)。

[0151] そして、機器10a及び機器10bは、吸 時間報告信部12に搭包されている共通機のうち、機器 10a又は機器10bとの間で用いる共通機を選定し、 その違定された共通機を用いて機器10a又は機器10 bに右する情報データを送受信する。

[0152] 図15~図17は、機器10a及び機器10bが両機器10a(10b) 間で使用する器能特徴の 強定順序を時来列で示したものである。以下の手順は、 時来列により取得指徴アーブルに結びされている共通鍵 を用いて通信を行うことを示したものである。

【0153】図15及び図16に示すように、機器10aが、取得指機器投館12に器積されている共通離Kn-1を用いて機器10bとの間で通信を行う(S401a)には、先ず、機器10aが、他の機器10bに対して、使用することが可能な共通離(Kn-1~Kn-3)の類別字(n-1~n-3)を送信するステップを行う(S501a)。

[0154] 具体的には、先ず、操作部11 (機器10mにある操作部11)が、ユーザの操作により機器10 bとの間で認証を行うための機器認証命令信号を検知した場合は、操作部11は、その検知した機器認証命令信号を検打13へと出力する。

【の155】そして、機作部11から機器器証命合信号が入力された模型器が入力された使用について、大力された機器器証命合信号を強定部15に出力し、取得情報管理部13から機器器証命合信号が入力された確定部15には、人力された機器器監命令信号に基づいて、機器器監命令信号に基づいて、機器器監命令信号に基づいて、機器器監

20

29 信号に対応する認証均衡の鑑別子 (n-3, n-2, n-1, n) を取得情報指視節 1.2から取得し、その取得した観 別子 (n-3, n-2, n-1, n) を通信師 1.4 へと出力す

(0156) その後、取得价格理部13から職別子(n-3, n-2, n-1, n) が入力された通信部14は、入力された職別子(n-3, n-2, n-1, n)を機器10bの通信部14へと送信する。一方、機器10bは、上記手順と同様に、機器10bの収得价報帯包部12に帯信されている職別子(n-3, n-2, n-1)を、職別子(n-3, n-2, n-1, n)を送信した機器10aに送信する(S501b)。

【0157】次いで、機器10aは、自機の取得情報器的 12に蓄積されている線別子 (n-3, n-2, n-1, n)と、機器10bから受信した線別子 (n-3, n-2, n-1)とを比較し、両者が一致している場合は、機器10bに遂信する関級データを暗り化する (S503a~S

[0158] 具体的には、機器10aにある過俗部14が、過信能25から模別子 (m-3, m-2, n-1) を取得し、その長程した機別子 (m-3, m-2, n-1) を単定部5 c~と出力する。そして、過信第14aから模別子 (m-3, n-2, n-1)が入力された単径部15cは、自機が使用する状態軽Kに対応する鍵別子 (m-3, n-2, n-1, n)を製む指摘指指数部12から吸引し、その原外し、種の機能を表現的12から吸引し、その原外した鍵

別子 (n-3, n-2, n-1, n) と、通信部14から入力された羅別子 (n-3, n-2, n-1) とを比較する。 【0159】 両者の臨別子を比較すると、両者の臨別子

(0.15.9) 四十の銀列子を比較すると、加右の銀列子(n-3, n-2, n-1) は、一致しているので、遊ば雨15 c は、対象人は、その一女している経別子(n-3, n-2, n-30-55, 右参単程下が一部段を観別子n-1を過ばする。また、この観別子n-1の道はは、撮影10トにある道定節15 c でも、上記回線の手順により行われる(3 80.3 b ~ 8.5 0.5 b)。このため、観彩10トにある道に節15 c は、右参回展下が一部段や観彩子n-1を確定することになる。

(0160) その後、韓別子n-1を確定した遠定師15cは、遠定した韓別子n-1に対応する共通館Kn-1を、欧科信報告報館12から取得し、その取得した共通館Kn-1を開催的12から取得し、その取得した東部間16からに送信する。そして、強定間16から送信する。日本には、大力された共通機Kn-1を用いて、機器10から送信する。では与化された情報データを確認10から送信する。「0161 更に、機器10から表通館Kn-1で時分でも大点館Kn-1で時分でも大点館をKn-1で時分でも大点館をKn-1で時分でも大点の影響につらの認識問26に、表現に大き雄型Kn-1で時分にそれた情報データを、自機が有する数別分子に対応できれた情報データを、自機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、日機が有する数別分子に対応できれた情報データを、現場する(S506a、S507a、S506b、S5

杉用2003-101533

9

30

[0162]次いで、機器10nが、吸得信仰を一プル12nにある認証信仰のうち、行が原根の別れた共通報Kn-3を検出するステップを行う (S402n)。 具体的には、行効即保判所信15nが、認証信仰に合まれる行効即提信報に入って、収得信仰を一プル12nにある認証信仰のうち、行効期限が別れた共通理Kn-3を検知し、その検知したことを示すよ通難検知に少を設算信仰

**は、必ずしも複踏10mと複器105回の適応の状態には依存しない。国時共適職氏の存効原味が別れると地類** 

2

されたときに行われる。

[0163]そして、イ労ש限判所部15mから共適難後が信号がスカされた県得指衛管側部13は、人力された未通職会が同分に基づいて、新しい、近過機を製味するための未過難要求同分を適信第14~と出力する。その後、イ勞ש限判所第15mから未過難要求信号がスカされた通信第14は、入力された共過難要求信号を認能管理第20~と送信する。

[0164] 高、総経債権(共通股K)は、定期的に出 成されるものである。14体的には、総轄債権出成部22が GPU (因示せず)で作組されている時間債権(時減)に 基づいて総額債権を送次生成し、その生成した総額債権 を総轄債額数債額3に滞債する(3401c)。

10165] 次いて、総証符照間20が、機器10nからの受染により、S401cで生成済みの所しい場面組 Knを機器10nに送信するステップを行う(S402 c、S701n~S704n)。以体的には、適信第1 4から共通健災米信りを受信した総証行理師20は、受信したよ道健災米信等1 5。そして、通信部25から共通健災保守が入力された経験情報で24人と出力する。そして、基連健災米信号に対応する時間25人と出力する。そして、経際情報管理部22から共通健Knを破除情報有限25からよるとし、が然情報管理部25から共通健Knが方式力された通信部25と、人力された共通健Knが充、地が入力された通信部25は、人力された共通健Knが、

適種要米信りを送信した機器10mに送信する。 10166] 更に、器能管理部20から共通難Knを受 信した機器10nの適信部14は、受信した共通鍵Kn を収得債報管理部13~と出力し、適信部14から共通 鍵Knが入力された吸得債額管理部13は、入力された 共通鍵Knを収得債額等的同13に署付する。ここで、 秘密情報管理部22は、入力された共通鍵Knを、行効 期限が長い順に群債する(同図の収得情報で、イが 即限が長い順に群債する(同図の収得情報で、イが に、収得情報で一ブル12㎡、から開発してもよい。 10167] 次いで、吸得情報を一ブル12㎡、を行す b) は、以下の手順により行われる (このS402nの)

20

**る機器10mと吸得値格テーブル12トを有する機器10mとの回の通信(3402m、3701b~3703** 

別子 (n-2, n-1, n) と、通信部14から入力された数 子 (n-3, n-2, n-1) が入力された強定部15cは、自 n) を取得情報番組部12から取得し、その取得した観 | 0 1 6 8 | 具体的には、先ず、機器1 0 n にある通信 を取得し、その取得した益別子 (n-3、n-2、n-1)を登 **伝色15c~と出力する。そした、通信毎14nから模型 手順は、S4018の手順と基本的には同様である)。** 部14aが、極路10bから観別子 (n−3, n−1) 機が使用する共通館Kに対応する額別子(n-2、n-1、 別子 (n-3、n-2、n-1) とを比較する。

限でが一番及い観別子ローを強定する。また、この観別 その一致している観別子 (n-2、n-1) のうち、有効期 子n-1の難定は、機器10bにある難定部15cでも、 【0169】 Jih の観別子のうち、観別子 (n-2, n-1) は、一致しているので、強定部15cは、例えば、 上記回様の手順により行われる。

n-1を路証即16~と出力する。そして、遊定部15cか 【0170】その後、観別子n-1を強定した強定部15 取符替数指位的12から収得し、その取得した共通額K **や、自復が行する観別子F1に対応する共通額Kn−1を用** いて復号化し、機器10gから送信された情報データを ら韓別子n-1に対応する共通離Kn-1が入力された認証 節16は、入力された共通職Kn-1を用いて、機器10 【0171】そした、破路10gかの共通鍵Kロー1や貯 cは、協定した機別子n-1に対応する共通機Kn-1を、 bに送信する情報データを暗号化し、その共通鍵Kn-1 で昨号化された信仰データを機器10bへと送信する。 り化された情報データを受信した機器10bの點証部 は、安信した共通職Kn-1で暗号化された信報データ 収得する。

[0172] 次いで、機器10bが、取得情報テーブル 1.2 bにある認証情報のうち、有効期限の切れた共通健 Kn-3を検出するステップを行う (S401b)。 具体的 には、有効期限判断部15gが、認証情報に含まれる有 **多類吸位数に基ムされ、取得信頼アーブル126にある** し、その倹知したことを示す共通建倹知信号を取得情報 陽監情報のうち、有効期限が切れた共通鍵Kn-3を検知 管理師13~と出力する。

険知信号が入力された取得情報管理部13は、入力され [0173] そして、有効期限判断部15aから共通数 た共通単検知信号に払づいて、新しい共通観を要求する ための共通盤熨水信号を通信部14~と出力する。その 後、有効期限判断部15aから共通健要求信号が入力さ れた通信部14は、入力された共通健要求信号を認証管 理師20へと送信する。

とができなくなる。

た共通要求信号を秘密情報管理部24~と出力する。そ から共通要求信号を受信した認証管理部20は、受信し 【0174】次いで、認証管理部20が、機器10bか テップを行う (S403c)。 具体的には、通信部14 らの夏米により、共通館Knを腹路105に送信するス

通信部25から共通要求信号が入力された秘密情 から取得し、共通難Knを通信部25〜と出力する。そ 通信部25は、入力された共通鍵knを、共通健要求信号 して、秘密信報管理部22から共通鍵Knが入力された 共通要求信号に対応する共通数Knを秘密情報書積部2. **報管理師24は、入力された共通要求信号に基づいて、** を送信した機器105に送信する。 【0175】夏に、認証管理部20から共通職Knを受 借した機器10bの通信部14は、受信した共通観Kn を取得情報管理部13~と出力し、通信部14から共通 b'を参照のこと)。尚、有効期限の切れた共通鍵Kn-3 **壁Knが入力された取得情報管理部13は、入力された** 秘密情報管理部22は、入力された共通録Knを、有効 **期限が長い順に蓄積する (同図の取得情報テーブル12** 共通観Knを取得情報指領部13に結積する。ここで、 は、取得情報テーブル126、から削除してもよい。

3 a) 。このステップ (S403a) は、上述したステ ップ(S401a)と同様の手順を行うので、ステップ 【0176】次いで、機器10aが、共通鍵Knを用いて 機器105との間の通信を行うステップを行う(S40 (S403a) の説明は、省略する。

点において取得情報テーブル12a (12b) にある共 **通鏈が異なった場合であっても、機器10g及び機器1** 0 bは、取得情報テーブル12a(12b)に蓄積され が、認証管理部20から新しい共通鍵を取得し、ある時 で、共通鏈が通信途中で更新されたとしても通信状態が 途中で途切れることなく、機器10g又は機器10bか た両機器に共通する共通鍵を使用することができるの [0177] これにより、機器10a及び機器10b ら情報デークを取得することができる。

**共通する共通健がなくなってしまった場合は、機器10** (10b) は、機器10bとの間で形成されていた無線 [0178] 一方、機器10aが、器配管理部20から 共通離を更新し続け、機器10gと機器10bとの聞で **る。このため、機器10gが、機器10gと機器10b** b)に共通の共通鍵を用いて情報データを送受信するこ a は、機器10 b との間で共通の共通鍵を有しないの で、機器10bとの間の通信を行うことができなぐな との間で共通の共通鍵を有しなくなり、両機器10m ネットワークが解除されるので、両機器10a (10 \$

得した共通鍵を取得情報デーブル12aに書館し、取得 **情報テーブル12aに蓄積されている共通鍵のうち、段** も古い共通鍵を削除することを示したものである。この 共通難Kを吸得する方法は、上述にも示したが、図18 に示す手順によっても行うことができる。同図では、機 器10が、認証管理部20から共通鍵を取得し、その取 [0179] 尚、機器10が認証管理部20から新しい 図17に示す具体的な内部動作(陽駐部16などの動 作)は、上配に示した動作と回接である。

8

校室2003-101533

た、熊袋ネットワーク内の情報ゲータがいつまでも外部 る第二路証信型の有効期限が切れれば、その盈曜された た各機器10は、無数ネットワークに似する機器が铬膜 【0185】このため、上記無礙ネットワークを形成し された場合であっても、その登職された機器10に有す 機器を無線ネットワークから排除することができるの

定の周期Trで時系列的に共通壁Kn-2、Kn-1、K

[0180] 同図の左側に示した認証管理部20は、

nを生成し、その生成された共通観Kn-2、Kn-1、

Knを順次送信する。認証管理師20から共通職Kn−

[0186] 災に、各機器10は、適定師15cが、他 位されている第二認能情報に含まれる機関子との間で基 通する値配数別子を抽出して、その抽出した値配数別子 の機器10が行する第二陽監情報に含まれる機関子を取 **得し、その取得した観別子と、取得情報階位師12に帯** も、各機器に共通の第二路配併報を選定することができ に対応する有効期限情報に基づいて媒有効期限情報に対 各世路10に複数の第二路監信組を行する場合であって **応する自動類二陽監信報を適定することができるので、** に溢れ出てしまうことを防ぐことができる。

0

[0181] 具体的には、遊定部15cは、秘密情報生成 **部22 (生成手段) で所定の周期毎に生成された第二賜証** 情報を複数取得し、その複数取得した第二點証情報の個 数が所定の個数を超えたときは、取得した複数ある第二 **認証情報のうちのいずれかを削除する。即ち、機器10** が同図中の時点1で受信した共通艇Kr-2は、時点3を継

過盤Kn−2、Kn−1、Knをそれぞれ吸料性数テーン

12a~12a'''に潜積されている共通健のうち、段

も古い共通離を削除する (S601~S603)。

5、Kn-1、Kn��の痘した抜路10位、夕疤した夫 ル12ョ~12a・・・に苦収し、その取得情報テーブル [0187] [第二次補形類]

20

ることができるので、内部に数配されている時計を用い

特定の周期Trが経過したときに所定の共通観を取得す

の有効期限は2Trとなる。これにより、機器10は、

【0182】(機器認証管理システム及び機器認証管理 方法による作用及び効果)このような本実施形態に係る

て共通键の有効期限を計測する必要がない。

過した後に取得情報テーブル12mから削除される。この ため、取得情報テーブル12gに蓄積されている共通館

4に時間付加部17とを有している点で相違する。この (機器器監管理システムの構成) 本発用の第二次施形態 施形値に係る機器器配管型システムの内部構造を示した ものである。同図は、第一実施形態に係る機器認証管理 相流する構造以外の構造は、第一英簡形態と同じである のか、相当する構造以外の構造についての観明は、治略 について図面を参照しながら説明する。図19は、本沢 路証管現前20に生成指示師27と機器10の通信師1 システムの内部構造 (図2参照) とほぼ向じであるが、

[0188] 第一次施形値では、適定師15cが、 認証 遊定部15cは、뭥駈管理師20から陽離損報を取得し どの認証情報を使用するのかを判断するものである。リ 情報(陽監情報の臨別子、共通難の有効期限、共通館) 報を使用するのかを判断していたが、本実施形態では、 た時間と、 吸得した関語情報の有効期限とに揺るいた、 体的な説明は以下の通りである。

20

筑一路監備報を有していない機器との間では通信を行わ

を行うことができない。このため、認証管理部20は、

ないようにすることができ、第一路監債報を有しない機

器10からの不正なアクセスを排除することができる。 [0183]また、第二點監情報を有する機器10は、 うことができないので、第二路監督報を有する他の機器 10との間では、その第二認証情報を媒介して無极ネッ トワークを形成することができる。このため、第二認能 **情報を媒介して無線ネットワークを形成した各機器10** することができ、秘密文書などの情報データが第二點証

は、第二路監信報を有しない機器10からの通信を排除

[0184]また、第二陽証情報には、第二陽証情報の 有効期限が含められているので、第二器証情報を媒介し て無礙ネットワークを形成した各機器10は、第二器証

**情報を有しない機器10に顕れることがない。** 

第二陽監督報を用いなければ他の機器との間で通信を行

機器10は、認証管理部20から予め取得した第一認証 **情報 (マスタ壁M)を用いて路監管理部20との間で通** 

機器認証管理システム及び機器認証管理方法によれば、

借をするための認証を行うので、前配第一認証情報 (マ スタ雄M)を有しなければ陽骶管理部20との間の通信

して、秘密情報の生成を所定の周期毎に指示するための る。生成指示部27から生成借号が入力された秘密情報 ように、所定の周期TFが経過した場合は、秘密情報生 生成師22は、入力された生成信号に基ろいて、婚れな状 [0189] 生成指示部27は、秘密情報生成部22に対 ものである。具体的に生成指示師27は、図20に示す **通顧Kを生成し、その生成した共通館Kを生成指示師2** 成部22に共通鍵を生成させるための生成信号を出力す 40

[0190] 道、回図に守ず共通第KI~K5点、多を存 って順次人力された生成信号に基づいて、その生成信号 樹生成都22が、生成指示師27から特定の周期TFをも に対応して順次生成された共通鍵を意味するものであ

7~と川力する。

20

8

きないこととなる。

0を盗難した者は、第二認証情報の有効期限が切れれば

クから排除することができる。また、第二路監備報を有 する機器10が盤簾された場合であっても、その機器1 第二認証情報を有する機器との間で通信を行うことがで

**情報の有効期限が切れた機器10を前配無線ネットワー** 

壁K1, K2が入力された通信部25は、入力された共通 なく生成指示部27からの生成倍号に応じて無条件に共 秘密情報器預期23に蓄積する。生成指示部27から共通 共通難K1,K2を通信部25に出力し、暗号化した共通 [O 1 9 1] 第密哲報生成部22から共通職K1~K5が入 **力された生成指示師27は、機器10gの要求とは関係 邸26へと出力すると共に、入力された共通額K1~K5を** 雌K1、K2をマスタ鍵Mで暗号化し、その暗号化した 通牒K1、K2(ユーザから熨状された共通額)を認能 壁K1、K2が入力された認証部26は、入力された共通 壁K1, K2を機路10にある通信部14〜と送信す

[0192]時間付加部17は、通信部14が認証管理 取得情報管理部13~と出力する。時間付加部17から 第20から第二路証情報を取得した時間を、第二路証情報 に付加する時間付加手段である。具体的に時間付加御1 時間情報を付加した共通観K1、K2が入力された取得 7 は、通信部25から共通職K1、K2を受信した場合 情報管理部13は、入力された共通鍵K1、K2を取得 を付加し、その時間情報を付加した共通観K1、K2を は、その共通額と1、K2を収貸した時間(時面控整) 情報器質問12に器積する。

20

成部22で生成された時刻に機器10の電源が入っておら (K1、K2) が生成された時点と比較すると多少超短 [0193] 尚、図20に示すように、秘密情報生成部 TdLている。この遊姫Tdが生する嬰囚は、認証管理 第20と機器10との間で行われる通信開始手順に時間 ず、機器10が認証管理部20に対して共通鍵を要求す 22で生成された各共通難(K1、K2)を通信第14で がかかること、通信網が混雑していること、秘密情報生 受信するタイミングは、秘密情報生成部22で各共通観 ることができない状況にあることなどが挙げられる。

[0194] 遠近部15cは、まず各共通難 (K1, K **去する (K2だけが除去されK1が残る場合と、K1と** る)。次に、残された共通鍵の中から時間情報が最も遅 い共通額を踏定する(つまり、KIだけ扱っている場合 はこれが遺ばれる。 KIとK2の両方が残っている場合 2)を闘べ、時間情報から1/21r組造しているものを除 K2のどちらも除去されず役る場合場合が考えられ はK2が選ばれる。

た共通数 (K1、K2) のうち、時間情報 (認証管理部 【0195】尚、確定部15cは、時間付加部17時間が 20から取得した時刻)が早い共通館K1を選定するこ 付加された第二點証情報(認証情報)を複数取得し、そ ら、付加された前部時間に基づいて、鞍時間に対応する 一つの第二認証情報を確定する第二確定手段である。 具 体的に選定部15cは、取得情報管理部13からの指示に より、取得情報器積部12に潜積されている時間情報が **行加された共通額(K1、K2)を取得し、その取得し** の前記時間が付加された複数ある第二認証情報の中か

【0196】(機器認証管理システムを用いた機器管理 路路監管理方法は、以下の手順により実施することがで きる。高、機器10が撤産部15~で強定された共通艦K 方法)上記構成を有する機器認証管理システムによる機 を用いて他の機器10に情報データを送信する方法は、 上配第一実施形態で述べた方法と同様に行われる。 【0197】 (1) 機器10a及び機器10bに有する **造定部15cが、それぞれ認証管理部20から同じ時間で** 取得した各共通銀 (K1、K2)を適定する場合

(106)にある遠定部15cが、認監管理部20から同 図21は、機器10 a (10b)が、 器配質理部20か **の厄フ時回や吸谷した共通際(KI~K2)を示したタ** 同図に示したタイミングチャートを用いて、機器10g **じ時間に取得した各共通鍵(K1、K2)を、時間付加** 第17で付加された時間に基ろいて強定する方法についる イミングチャートを示したものである。以下の手順は、 て以下説明したものである。

て、生成指示師27から生成信号が入力された秘密情報 生成部22は、入力された生成倡号に基づいて、新たな共 **通鍵K1~K5を生成し、その生成した共通難K1~K** 【0198】先寸、秘密情報生成部22が、所定の周期T 生成指示部27が、図21に示すように、所定の周期T r が経過した場合は、秘密情報生成部22に共通難(K1 ~K5)を生成させるための生成信号を出力する。そし r 毎に共通鍵を生成するステップを行う。具体的には、 5を生成指示部27~と出力する。

管理部20にある認能サーバ初期設定により(図20の左 **端時刻) 複数同時生成もすることができる) を送信する** ステップを行う。具体的には、秘密情報生成部22から共 通難K1~K5が入力された生成指示部27が、入力され た共通鍵K1(ユーザから要求された共通館)を認証部2 (104)に対して、矩かに出成された共通艦K1(本 実施形態では、共通難は10ず0生成しているが、認能 6~と出力すると共に、入力された共通録K1~K5を秘 [0199] 次いで、認証管理部20が、機器10a 密信報蓄積部23に蓄積する。 30

る。この場合、共通難は秘密情報器積部23から取得さ [0200] 尚、認証管理部20は、機器10a (10 b) からの要求等により共通鍵を送信することもでき れ、認証師26に出力されます。

に出力し、暗号化した共通鍵K1が入力された通信部25 鍵Mで暗号化し、その暗号化した共通観K1を通信部25 は、入力された共通難K1を機器10にある通信部14 【0201】そして、生成指示部27から共通鍵K1が 入力された認証部26は、入力された共通鍵K1をマスタ

理部20から受信した共通鍵K1に基ろいて、時間情報 [0202] 次いで、機器10a (10b) は、認証管 を付加するステップを行う。具体的には、時間付加部1

へと出力する。そして、時間付加部17から時間情報を 7 が、通信部25から共通職K1を受信した場合は、そ の共通額K1を収価した時間(時間積盤)を付加し、そ の時間情報を付加した共通録K1を取得情報管理部13 付加した共通鍵K1、K2が入力された取得情報管理部 13は、入力された共通艇K1、K2を取得情報器積部

からの指示により、取得情報書積部12に蓄積されてい ータイミングも間では、機器10g及び機器10b間で 行われる情報データの通信を両者に共通する共通健K3 入力された場合は、遠定部15cが、取得情報管理部13 し、その吸仰した共通難(K1、K2)のうち、上配手 に示すように、 認能管理部20から取得した共通館 (K り、回図中のタイミングョータイミングも叫で使用する [0203] その後、操作師11に機器踢駐命合信号が このため、機器10g及び機器10bは、タイミングg 【0204】尚、機器10a及び機器10bは、図21 共通鍵K3が両機器10a(10b)で共通している。 る時間情報が付加された共通館 (K1、K2)を取得 1、K2、K3) の取得時間 (時間情報) が同一であ 頃に従って10を強択して認証部16~と出力する。

20

を用いて行うことができる。

機器10cに有する遺定部15cが、それぞれ認証管理部 を用いて機器10a (10b) 間で通信を行うことを示 健の取得時間 (時間情報) と、機器10cが認証管理部 20から取得した共通鍵の取得時間(時間情報)との間 【0205】尚、図22及び図23は、機器10a及び したタイムチャートである。図22中に示されているT 20から異なる時間で取得した各共通難(K1、K2) D1は、機器10 aが認証管理部20から取得した共通 の時間差を意味するものである。

の間で共通盤K3を使用することができるまでの時間は 1/2Tr-TD1である。このため、機器10aは、上配1/2 ば、自機が機器10cに対して情報データを送信するこ [0206] 同図に示すように、機器10cが、認能管 **単部20から共通額K3を収得してから、機路10m**と Tr-TD1により、TD1が1/2Trよりも大きくなれ とができない時間が生じる。 [0207] 従って、この場合、機器10aが機器10 cに対して情報データを送信する際には、機器10cに めに、共通難K3を使用する時間を、図中のp点より1/ す) する。これにより、タイミングョータイミングも間 における共通鍵K3が、機器10aと機器10cとの間 **か回じへなり、被略10gと概略10cは、共通解K3** を用いて情報データを送受信することができる。尚、機 は、機器10gで使用される共通難K3に対応させるた 2Tr早めるように散定(以下、単に「マージン」と略 ある過定部15cは、タイミングョータイミングも叫で 機器10aとの間で情報データを送信することができ 器10cは、上配Td1が1/2Trよりも小さければ、

将原2003-101533

8

についてのタイミングチャートを示したものである。上 **割内容と同僚に、機器10cは、タイミングcータイミン** /2Trよりも大きくなれば、自機が機器10mに対して る。 【0208】また、図23は、図22とは逆に、機器! 0 cが、機器10 nに対して信徴ゲータを送信する場合 **グ d 側では、図 2 3 中の1/2 Tr - T D 2 に よ り、 T D 2 が 1** 情報デークを送信することができない時間が生じる。

**めに、共通額×3の仮出や様にする時間か、図中の4点** ン」と略す)する。これにより、タイミングゥータイミ a に対して信根データを送信する際には、機器10 n に は、機器10cで使用される状態機K3に対応なせるた 【0209】従りて、この場合、機器10cが機器10 ング4回における共通額K3が、破路10gと破路10 c との回で回じくなり、極路10 nと極路10 c は、状 る。尚、機器10cは、止配Td1が1/2Trよりも小 さければ、機器10mとの川で情報データを送信するこ より1/2Tr遅らせるように歓迎(以下、中に「マージ **ある趣定部15cは、タイミングcータイミングd回で** 通額ス3を用いて控数ゲークを込み信することができ

9

n(10b)がn個の共通鍵を有する場合は、認能管理 1) [上手順の一般式]以上の時間が構造した秘密情報 のうち、最も新しい共通難を使用する。このため、機器 [0210] 東九、機器10n (10b) は、機器10 10m(10b) は、機器10m及び10bとの間で状 面鍵を取得する時刻に遊があるときは、共通観を使用す 及び機器105川で情報データを送受信することができ 「ケージン」の一袋式)のケージンがひえれば、苺粽ー O a (10 b) に有する共通値が等しくなり機器10 a 係20からn個の共通離を取得してから1/2Tr (nー ることができる時間に1/2T r (n — 1)時間(上記

30

【0211】図24は、無線方式Aと無線方式BとがW 式Bの機器10bとに有している共通壁の有効期限がほ なる場合でもったも、無极方式Aの破路10mと無极力 ぼ同等であることを示したものである。

[0212] 同図に示すように、無模方式Aの複路10 TAで更新されていくが、無极方式Bの複器10bに有 0 bでは、タイミングr時点での共通館の数を、上配機 している共通数(Kn1~Kno)の有効原限は、TAの 器10nの共通観数 (Kv1, Kv2の2つ) の3/2作であ 2/3倍の周期 (Tin) で更新される。このため、無缺方 式Aの機器10mでは、タイミング・時点での共通観 (Kai, Ka2) の数を2つとし、無縁方式Bの機器1 a に有している共通館(Kvi~Kva)の有効即限は、 A1. KA2) の有効期限と機器10bの共通壁 (Kii. KB2)の有効原限とは、ほぼ问一になる(何図中の" る3つ (Kn1, Kn2, Kn3) にすれば、共通館 (K

△し"は、機器10mと機器10bとの共通鍵の行効関

2

3

【図4】本発明の第一実施形態における機器が認証管理 **郭から共通鍵を取得するまでの概念図(1)を示したも** [図5] 本発明の第一実施形態における機器が認証管理

限差が微差であることを意味している)。

【0213】従った、張路10 n (10 P) の共通額の 随の数を設定すれば、ほぼ同一に扱うことができる。ま た、各機器10g(10b)は、異なる無線方式が採用 されている機器10g(10b)の共通鍵や、その共通 鍵の数が異なる場合であっても、上記に示すタイミング 吹いは機器105にある共通壁の一部を削除した場合で あっても、上記のような更新周期(T.A. T.B.)、共通 **育効期限は、機器10gにある共通館の一部を削除し、** で共通鏈を更新することにより、各機器10g(10

節から共通鍵を取得するまでの概念図 (2) を示したも 【図6】本発明の第一実施形態における機器が認証管理

のである。

【図7】本発明の第一実施形態における認証管理部が複

数の通信方式を採用した機器を管理していることを示し [図8]本発明の第一実施形態における機器の状態避移

た図である。

部から共通鍵を取得するまでの概念図 (3) を示したも

のである。

9

[図9] 本発明の第一実施形態における機器が認証管理

を示した図である。

部から共通鍵を取得するまでのフローを示した図であ

機器の登録情報を削除するまでのフローを示した図であ [図11] 本発用の第一実施形態における機器が複数あ る共通鍵のいずれかを用いて他の機器との間の認証を行 【図12】本発明の第一実施形態における機器が他の機 器間で共通健を用いて認証が行われるまでのフローを示 【図13】本発明の第一実施形態における一つの機器が

20

うことを示した図である。

【図10】本発明の第一実施形像における認証管理部が

記時間を用いることによっても第二路監情報を選ぶこと 認証管理システム及び機器認証管理方法によれば、適定 年段から第二路監督権を取得した時間)に基づいて、そ お、第二點指位は、第二點指位はのをががが</ ができる。このため、各機器は、各機器間で有する第二 **認証情報がある時点で異なる場合であっても、第二認証** [0214] (機器認証管理システム及び機器認証方法 による作用及び効果)このような本実施形態に係る機器 部15cは、時間付加17で付加された時間 (認証管理 情報の時間情報に基づいて各機器に共通する認能情報を の時間に対応する第二點監情報を遵ぶことができるの

[0215] この実施形態により、各機器は、通信開始

2に潜程されている第二認証情報に含まれる裁別子との 間で共通する値記載別子を抽出して、その抽出した類別 対応する一つの第二認証情報を遊定することができるの が同一でなくても(認証情報の有効期限の終了時期が現 時に諡別子信頼をやりとりする必要がないため、例えば 802.11のような、通信の受信者数が複数ある場合 (不特定多数である場合) でも認証情報を遊ぶ手段を得 理システム及び機器認証管理方法によれば、各機器10 が、他の機器10が有する第二認証情報に含まれる難別 [発明の効果] 以上説明したように本発明の機器認証管 子に対応する有効期限情報に括ろいて数有効期限情報に で、各機器は、曳時点において各機器に有する認証情報 子を取得し、その取得した難別子と、取得情報蓄積部1 ち、各機器間に共通するいずれかの認証情報があれば、 なる場合でも)、各機器に有する複数の認証情報のう [0216]

【図1】本発明の第一実施形態に係る機器認証管理シス

|図2| 本発用の第一実施形態に係る機器認能管理シス

b) にある共通鍵の有効期限をほぼ同一にすることがで

したものである。

**旭の機器との間で通信を行うための認証を行うことがで** 

# [図面の簡単な説明]

アムの観略構成を示すブ観略図である。

テムの内部構成を示すプロック図である。

【図14】本発明の第一実施形態における複数の機器が 複数の共通键のいずれかを用いて認証を行うことを示し

他の複数ある機器との間で認証を行うことを示した図で

30

た図である。

【図15】本発明の第一実施形態における機器が認証管 理部から共通難の更新を受けたときに他の機器間で行わ れる悶証を示した図である。

【図16】本発明の第一実施形態における機器が他の機 器との間で行われている通信を行うまでのフローを示し た図である。 【図17】本発明の第一実施形態における機器が認証管 理部から共通離を更新したときに他の機器との間で通信 を行うまでのフローを示した図である。

40

【図18】本発明の第一実施形態における機器が認証管 理部から共通鍵を更新するまでのフローを示した図であ

【図19】本発明の第二実施形態に係る機器認証管理シ ステムの内部構造を示した図である。

【図20】本発明の第二実施形態における機器が認証管 **理部から所定のタイミングで共通鏈を取得していること** を示した図である。

-21-

20

【図3】本発明の第一実施形態における認能部のOSI

8

校屋2003-101533

|図21| 本発明の第二実施形態における複数の機器が **認証管理部から共通鍵を所定のタイミングで取得してい** ることを示した図 (1) である。

[図25] 従来における家邸内無数ネットワークを示し

【作号の説明 た図である。

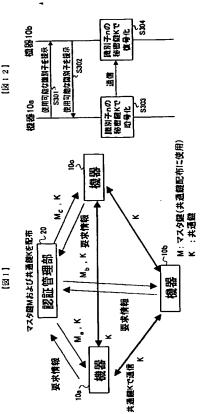
証管理部から共通鍵を取得したことを示した図である。

認証管理部から 共通鍵を 所定の タイミングで 取得してい [図23] 本発明の第二実施形態における異なる通信方 [図22] 本発明の第二実施形態における複数の機器が ることを示した図(2)である。

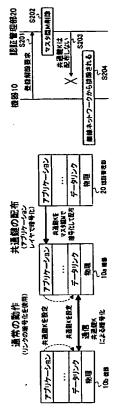
【図24】本発明の第二実施形態における異なる通信方 式を採用した複数の機器が陽監管型部から共通鍵を所定 式を採用した複数の機器がそれぞれ異なる更新期間で認 のタイミングで取得していることを示した図である。

c…強定部、16…髂骶部、20…髂監管期間、21… 3…取得价模管理部、14…通信部、15…認証价如決 定部、15m…有効即限判時間、15p…順序間、15 部、24…秘密情報管理部、25…通信部、26…路賦 10…機器、11…操作師、12…取得情報器損師、1 操作部、22…秘密情報生成部、23…秘密情報器情 9

[図12]

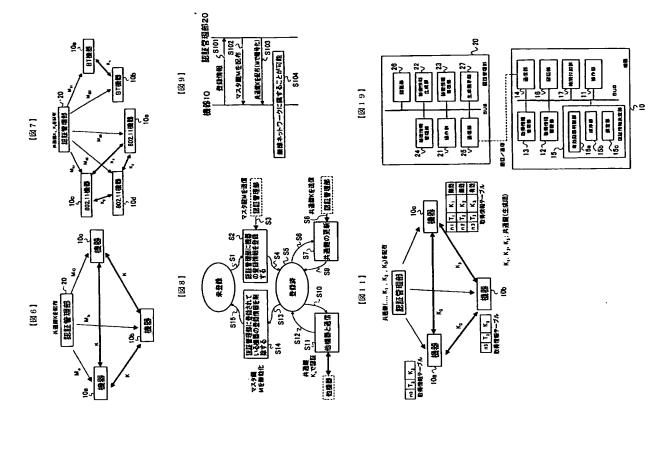


(区) (図 3



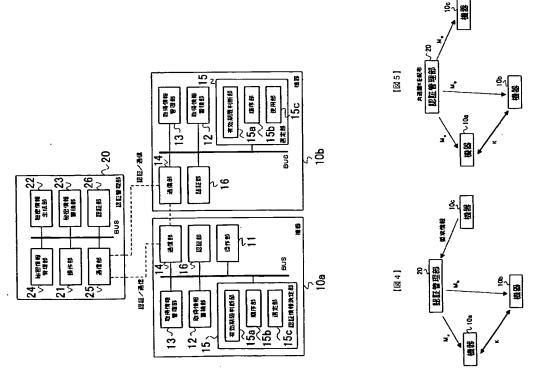
-25-

[図2]

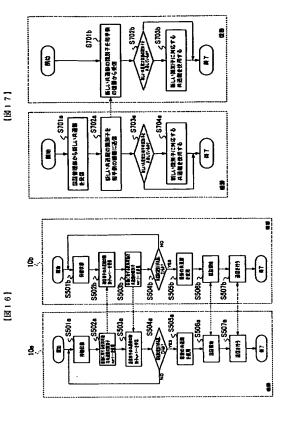


-24-

-23-



[図13]

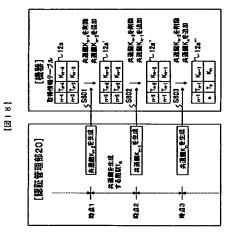


n-2 K<sub>n-2</sub> 額数 n-i K<sub>n-1</sub> 額数 c K<sub>n</sub> 数数 p能益額アーブル

ト共通銀Kaで暗号化

u W 機器 100

n-1 ス<sub>r-1</sub> 競技 n ス, 性数 反応室部ポープス [図14]

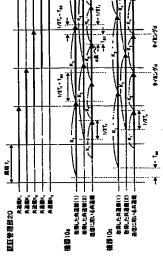


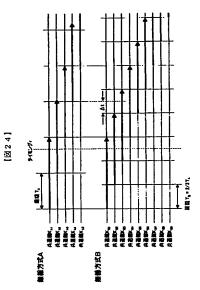
[図15]

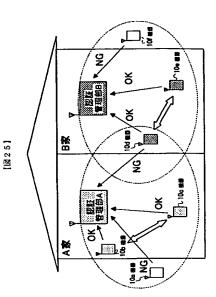
[18征管理部20]	[機器10a]	[機器100]
S4010	取事権報デーブル 0-9 Tr-3 Ke-3 し12a	<b>数は情報テーブル</b>  アコトップ Kp-3   ~12b
<b>共通關人長生成</b>	2	
S402c	大学の関係のデス	
本語観火・存役信	12a S402a	120 C-120
	<u>و</u> م	1 1 E
SAGG		大学の政策が大を選出
朱温和人长进位	0-27a-2 Km2 ~12a"	n-2 To-2 Kn-2 ~12b'
	n T <sub>n</sub> K <sub>n</sub> K <sub>n</sub> CEEE	17-1 Tr. 1 Krr.

-25-

-56-





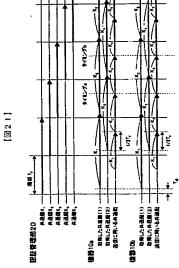


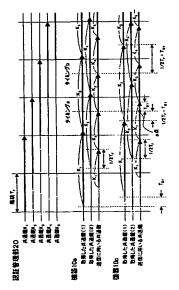
特開2003-101533

(2)

[図20]

比位管理部20





[図22]

-11-

-28-

フロントページの税ぎ

(72)発明者 協本 幹生神奈川県川崎市家区小向東芝町1番地 株式会社東芝研究開発センター内

ドターム(参考) 58085 AE13 AE23 5J104 AA07 AA16 EA06 EA18 KA02 KA04 KA09 MA01 NA02

-29-